www.hackerjournal.it n. 46

CODICE RUBATO
I PRIMI ATTACCHI

Allarme GPS
Siamo CONTROLLATI

NOKIA
PILOTIAMO
il cellulare

Groviera
WIRELESS
neanche WPA
è SICURO

Spiamo
la POLIZIA

TRUCCHI
diventare
un ALTRO

QUATTORDICINALE ANNO 3
11 MARZO 2004 - 25 MARZO 2004
SPED. IN ABB. POST. 70% - MILANO

EMERGENZA
DISTRUGGIAMO i DATI subito!

Anno 3 – N. 46
11 Marzo 2004 - 25 Marzo 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Bismark.it, Il Coccia, Gualtiero Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano
il 27/10/03 con il numero 601.

Codice rubato:

Tutto è iniziato lo scorso 12 febbraio, quando Microsoft ha emesso un comunicato stampa (http://www.microsoft.com/presspass/press/2004/Feb04/02-12windowssource.asp) per ammettere che una parte del codice sorgente di Windows è stata rubata e pubblicata su Internet.

I file sono due, uno che contiene una buona parte del codice di Windows NT4 e uno che contiene una frazione del codice di Windows 2000, approssimativamente il 15 percento del totale. C'è dentro codice di rete, tra cui winsock e inet, codice di shell e altri elementi compreso il codice del log degli eventi e perfino alcuni dei salvaschermo preinstallati. Su Internet sono arrivati in totale 30.915 file, per circa 13,5 milioni di righe di codice, di Windows 2000, e 95.103 file per 28 milioni di righe di codice per quanto riguarda Windows NT.

Tutto il materiale rubato gira per Internet dentro un file windows_2000_source_code.zip, di 213.748.207 byte

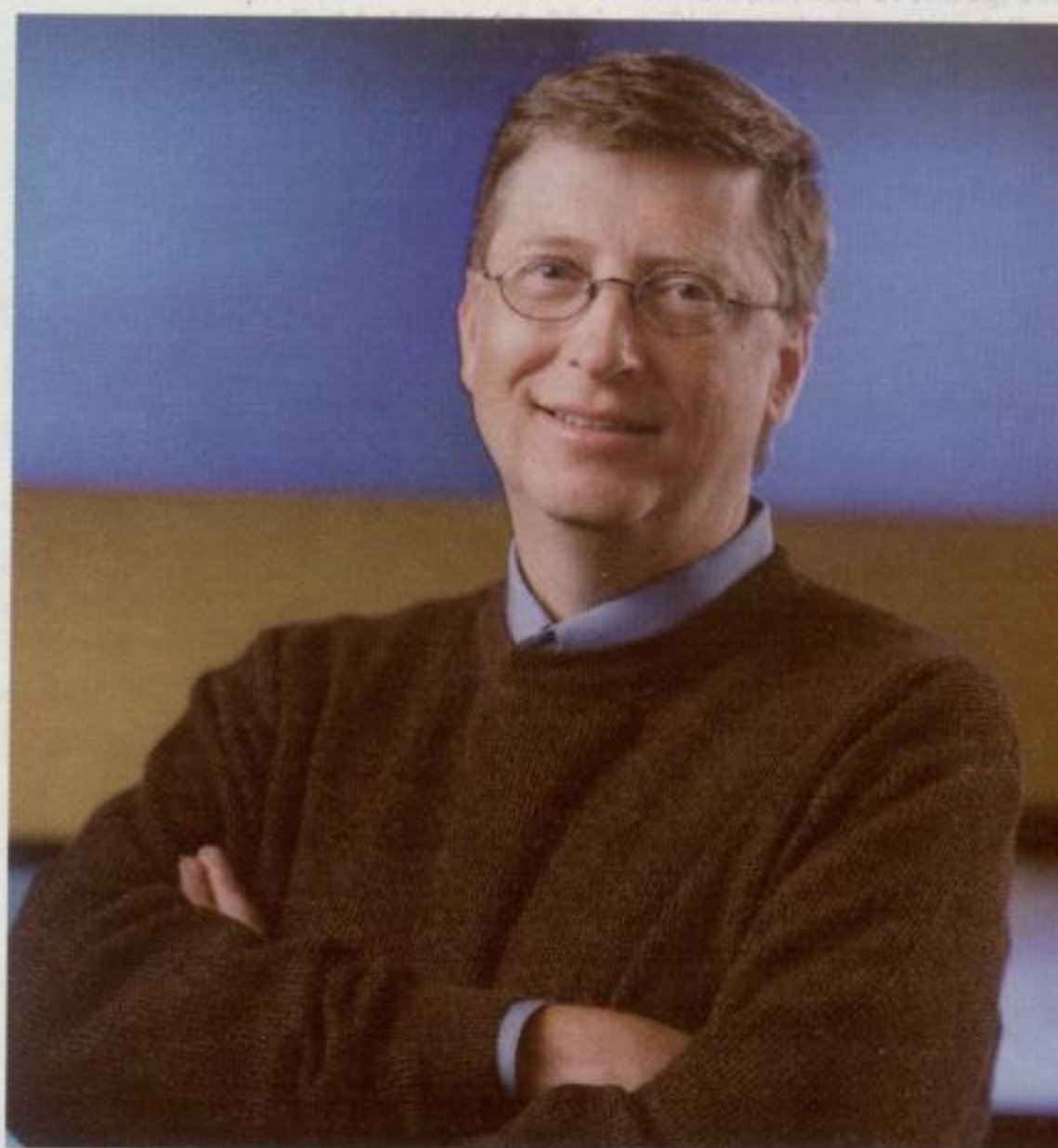
I file sono datati 25 luglio 2000, ma non sono vecchi come sembrano: lo sviluppo di un sistema enorme e confuso come Windows richiede anni. Tutto

INIZIANO gli ATTACCHI!

SAPPIAMO PRATICAMENTE TUTTO, anche che cominciano già i NUOVI ATTACCHI basati sul CODICE RUBATO

sta girando per Internet dentro un file Zip chiamato windows_2000_ source_ code.zip, di 213.748.207 byte. Qualche burlone ha già messo in giro file con questo nome e di questa lunghezza, che però contengono solo una lunga lista di zeri. Il file, decompresso, occupa circa 660 mega, praticamente un CD. A detta di Microsoft, l'intero codice sorgente di Windows occuperebbe circa 40 giga.

Il genio nella lampada

Microsoft sta cercando attivamente di rimettere il genio nella lampada, inviando lettere di minaccia a quanti vengono individuati nel mettere il file su Internet e postando avvertimenti su numerosi sistemi p2p. Nel frattempo è già cominciata l'analisi del codice. Per quanto piuttosto datato, è stata già trovata una falla in Internet Explorer 5, che tuttora molti usano. Non è per niente escluso che nel tempo possano arrivare altre minacce per Windows. La qualità del codice sembra piuttosto buona. Non

La prima volta nel 2000

Nel 2000 Microsoft ha denunciato l'ingresso di hacker all'interno della sua rete di computer. A detta di Steve Ballmer, amministratore delegato di Microsoft, gli accessi clandestini si sono susseguiti per alcune settimane e sono arrivati ad avere accesso a parte del codice sorgente di Windows, ma non è stato modificato niente, anche se in teoria qualcosa potrebbe essere stato copiato. All'origine del crack, probabilmente, il trojan Qaz (http://www.pchell.com/virus/qaz.shtml). A dire il vero era successo qualcosa anni prima, con la diffusione dei sorgenti di DOS 6.22, ma era codice così vecchio che nessuno se ne era realmente interessato.

▲ *Non succede solo a Microsoft. Il gioco Half-Life 2 ha subito un notevole ritardo nella pubblicazione proprio a causa di una diffusione non autorizzata di codice sorgente*

così la sua struttura; Windows appare pieno di pezze, messe in ogni dove per cercare di mantenere la compatibilità tra mille componenti e programmi diversi. Guardando il codice ci si fa una buona impressione dei programmatori Microsoft e una cattiva impressione di Windows.

Colpa di chi

Responsabile della situazione è ormai senza dubbio Mainsoft (http://mainsoft. com/), azienda da molto tempo partner tecnologico di Microsoft, di quelli che hanno accesso al codice sorgente in questione, e dai cui uffici è stato trafugato il codice, come testimonia un log di errore in esso presente, che fa riferimento all'indirizzo di un impiegato dell'azienda. Il computer Linux usato a scopo di sviluppo, da cui probabilmente è partito il codice, potrebbe essere stato usato da Eyal Alaluf, Director of Technology di Mainsoft, durante lo sviluppo di MainWin, un prodotto di Mainsoft. Fino a tre anni fa Mainsoft era una delle due sole aziende autorizzate a vedere i sorgenti di Windows. Ora la Shared Source Initiative di Microsoft consente a più soggetti (prevalentemente enti governativi e organizzazioni molto grosse) di sbirciare nel codice.

Guardando il codice ci si fa una buona impressione dei programmatori Microsoft e una cattiva impressione di Windows

▲ *Mainsoft è stata identificata da subito come la responsabile della "fuga di codice" a causa di un riferimento all'e-mail di un impiegato dell'azienda nascosto tra le righe*

◄ *Per ora la linea XP non è stata ancora toccata dai furti di codice. Domani, chissà*

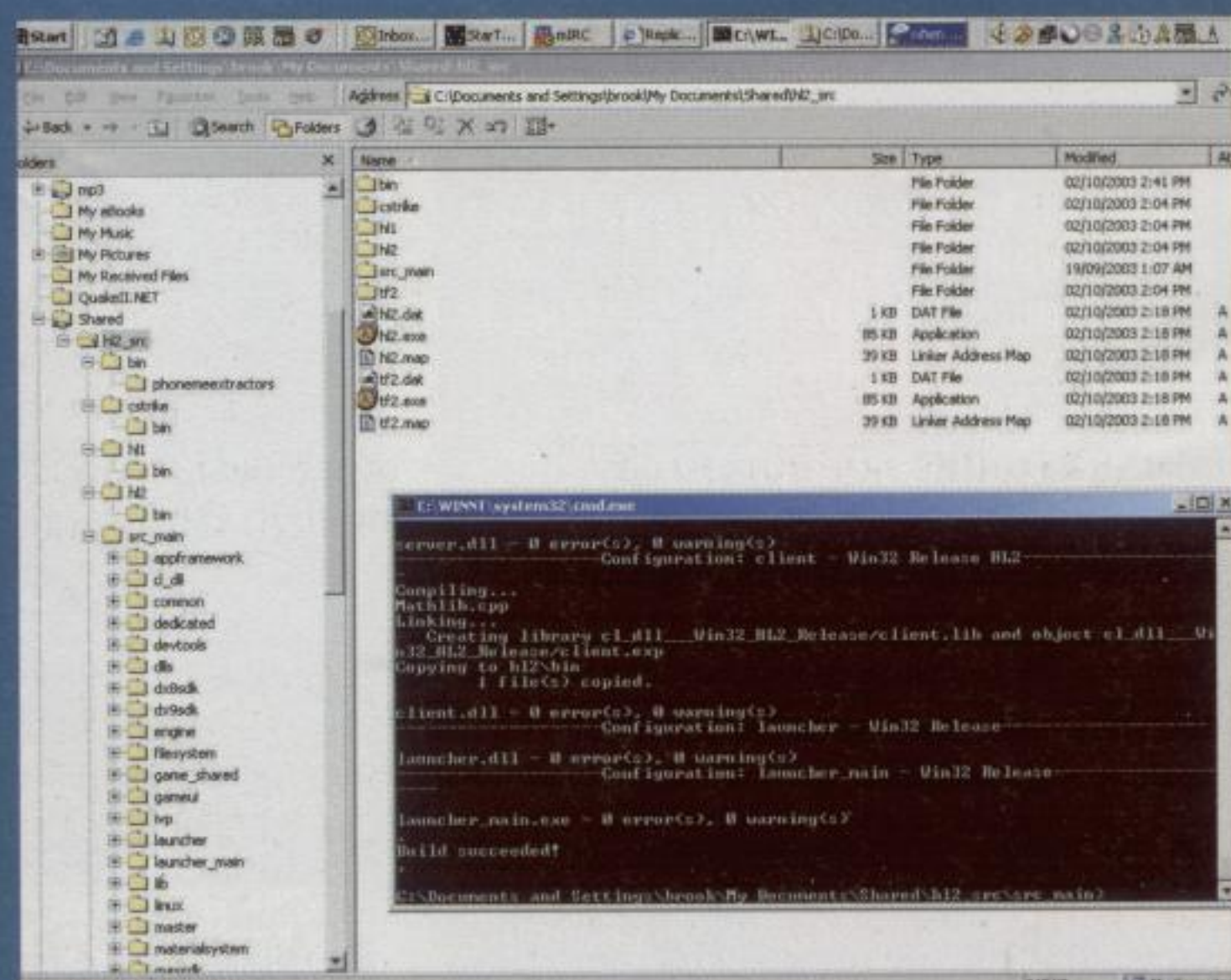
Il codice di Windows resta segreto, ma in molti hanno potuto iniziare a sbirciare dal buco della serratura. Molto meglio Linux, che è gratuito, aperto e osservabile in piena luce da tutti.

Reed Wright
reedwright@mail.inet.it

Dal codice rubato a una cattiva immagine

Un attaccante può creare una immagine bitmap che Explorer non riesce a leggere in modo appropriato, andando in integer overflow e permettendo l'esecuzione di codice ostile con gli stessi privilegi dell'utente bersagliato. Il bug affligge varie versioni di Internet Explorer e in particolare le seguenti:

IE5.01 SP1 5.00.2614.3500 su Windows 2000 Pro SP2
IE5.01 SP1 5.00.2920.0000 su Windows 2000 Pro SP2
IE5.01 SP2 5.00.3315.1000 su Windows 2000 Pro SP2

Si noti che sono tutte versioni di Explorer 5 (ormai aggiornato a 6) ma che Microsoft supporta la terza versione fino al 30 giugno 2004, come afferma la sua pagina http://support.microsoft.com/ default.aspx?scid=fh;%5 Bln%5D;LifeWin.
Questo bug è stato trovato analizzando il codice sorgente rubato e messo su Internet. Il file colpevole, per la precisione, è win2k/private/inet/mshtml/src/site/download/imgbmp.cxx. Per ora non esistono cure, a parte passare a Explorer 6.

freeHACKnet

La prima rivista hacking italiana

SAREMO DI NUOVO IN EDICOLA GIOVEDÌ 25 MARZO!

ACCOUNT@HJ.IT

Pop3 e Smtp da utilizzare per l'email di hackerjournal.it. Se preferisci consultare l'e-mail tramite il tuo client di posta elettronica (Outlook, Eudora, ecc...), ti ricordiamo i seguenti parametri da impostare:

pop: pop3.hackerjournal.it

SMTP: Devi usare i parametri che stai attualmente utilizzando per la tua connessione ad Internet.

Se per esempio utilizzi libero inserisci smtp.libero.it, se usi Tin mail.tin.it e se usi la nostra connessione usa smtp.hackerjournal.it.

Importante: come username devi inserire l'indirizzo di posta completo e non solo il suffisso.

HJ Collection #6

Se ti sei perso qualche numero di HJ approfitta della Collection! È in edicola la nuova Collection di Hacker Journal con i numeri dal 31 al 36 a soli 4,99 Euro.

Richiedila al tuo edicolante oppure scrivici all'indirizzo **edicola@hackerjournal.it** per sapere dove trovarla vicino casa.

Impostazioni FreeHACKnet

Se già possiedi un account @hackerjournal.it puoi usufruire degli stessi dati di username e password.

Dati per la connessione
Numero telefonico per la connessione: 7020005073

Username: la tua email (nome@hackerjournal.it)

Password: la tua password

Altri servizi
Server SMTP: smtp.hackerjournal.it
Server POP3: pop3.hackerjournal.it
Server NNTP: news.hackerjournal.it
Server FTP: ftp.panservice.it

Assistenza tecnica:
info@hackerjournal.it

Ricordiamo che l'e-mail si attiverà quando riceverà il primo messagio... quindi per attivarla basta mandare un e-mail al vostro indirizzo @hackerjournal.it

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete gli arretrati, informazioni e approfondimenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo!

USER: PUFFI

PASS: BUFFI

PASSWORD E .PWL

*Ciao, so che non c'è bisogno che ve lo venga a dire io, ma riguardo l'articolo della password di Windows non avete segnato che cancellando semplicemente il file *.pwl si può entrare in Windows senza dover inserire alcuna password. Mi chiedevo se potevate inserirlo nel prossimo HJ. Vi ringrazio!*

Tremors

Ecco fatto. Solo un appunto che vale per molti altri: quando scrivete una email (le leggiamo tutte, ma sono centinaia e non possiamo rispondere sempre!), scrivetela seguendo la netiquette. Ovvero evitando il maiuscolo, che è come GRIDARE! Ciao e grazie a te.

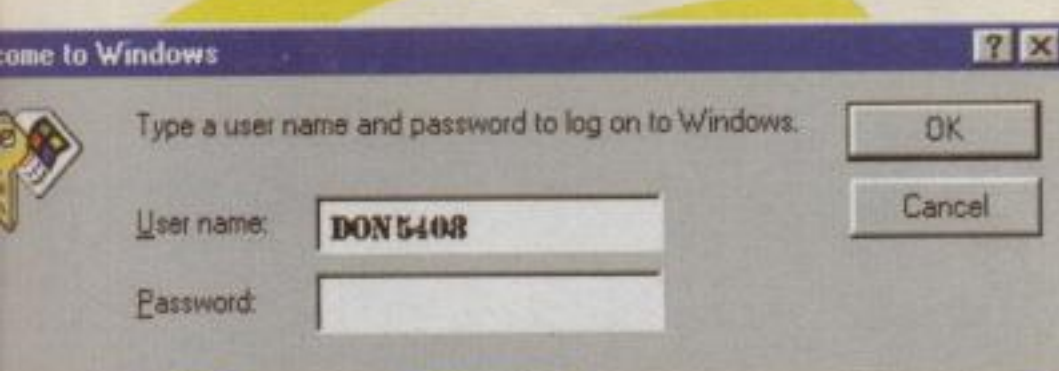
ome to Windows

Type a user name and password to log on to Windows.

User name: DON5408

Password:

OK

Cancel

▲ ***Oltre la barriera dell'inglese, c'è solo il Dizionario dei Dizionari. Vale la pena di fare il salto, no?***

SPETTACOLARE!

Carissima redazione di Hacker Journal,sono un vostro lettore novizio, devo dire che la vostra rivista è spettacolare!
Proprio perché sono novizio vi chiedevo gentilmente se potevate fare un articolo su tutte le sigle che si possono trovare su internet. Vi ringrazio in anticipo per la vostra gentilezza.

G1UL10

Un buon dizionario di Informatica e Internet comprende almeno 200 mila lemmi, e ovviamente non sono tutti. Supposto di riuscire a infilarne 50 per pagina, con relativa spiegazione, potremmo andare avanti per 4000 pagine, ovvero 125 numeri (scrivendo solo quello...). Ora, siamo d'accordo che la nostra rivista è spettacolare, ma non vorremmo che diventasse anche un po' monotona... ;) Scherziamo! Pensiamo che il metodo migliore sia quello di mantenere altissimo il livello di curiosità. Per esempio, ogni volta che incontri un termine che ti sembra di non conoscere, prova a fare una query (ricerca) su uno dei tanti motori (http://www.google.it, tanto per cambiare...) e leggi qualche riga. Magari in inglese, facendo un po' di fatica se non lo mastichi troppo. Dopo un po' ti accorgerai che, come per incanto, sia il tuo inglese, sia la tua conoscenza informatica è aumentata e ogni termine che avrai capito sarà un trampolino per comprenderne altri dieci.Se invece ritieni di cavartela con l'inglese, vai diritto su OneLook (http://www.onelook. com): è un metadizionario, che esegue ricerche su tutti i dizionari che lui conosce in Rete. C'è tutto, e anche di più.Da parte nostra cercheremo di non dare mai per scontato nulla e troverai sempre qualche articolo più semplice e qualche altro più per iniziati.
Non spaventarti, insisti.

OneLook

Dictionary Search

Word or phrase: hacker Search

Find definitions ○ Find translations ○ Search all dictionaries

- Enter a word to search for dictionary web sites that include that word.
- Enter a wildcard pattern to search for words. Valid wildcards are * (matches any sequence of letters) and ? (matches one letter).
- Examples: bluebird, blue*, *bird, bl????d, bl*snow
- New: Test out the reverse dictionary feature. ("A pain-free way to get that word off the tip of your tongue", says the USA Today.)

Featured Onelook sponsors: Shoes - ShoesBox, Shoes-Boots-Online Accelerator Download Online

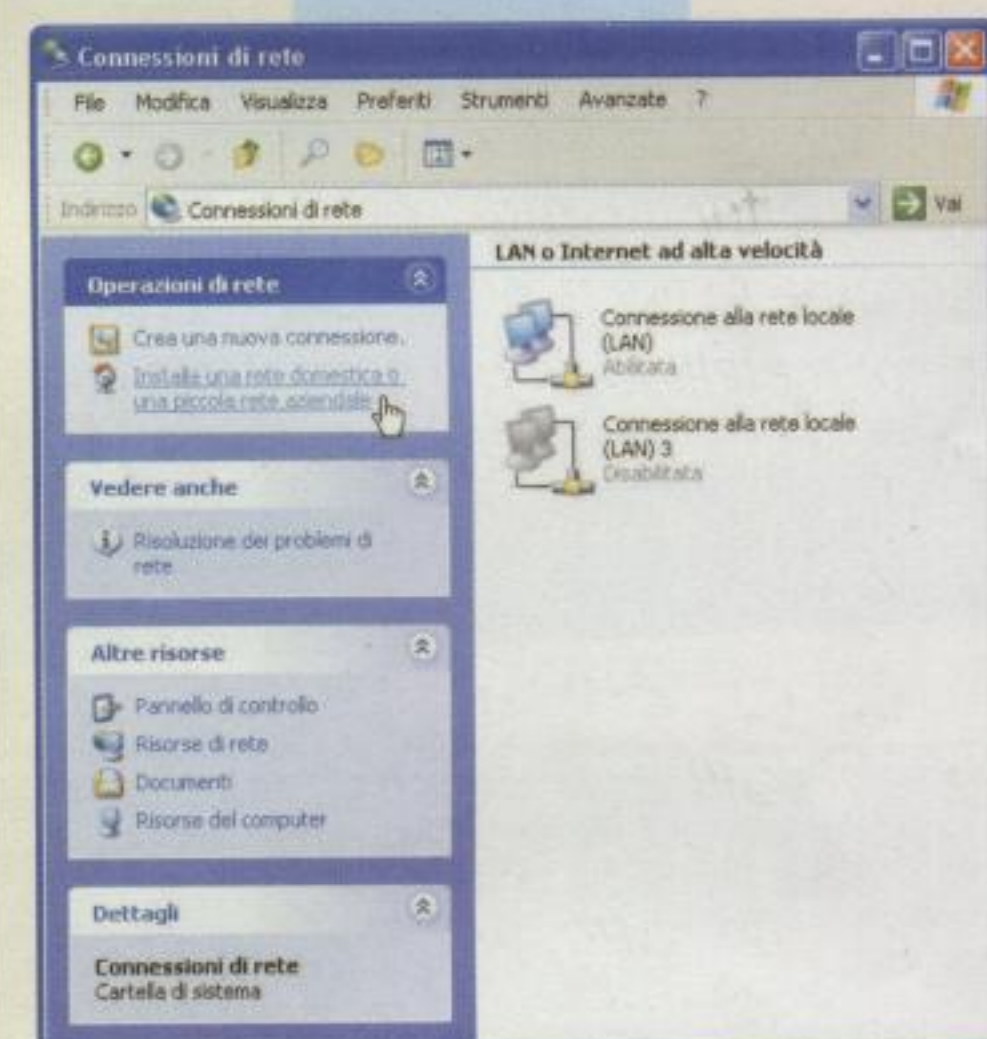
5,998,569 words in 964 dictionaries indexed

Link to us FAQ Privacy StudyTech.com Today's word is relevant

▲ ***A che cosa serve spendere tutti quei soldi per un antivirus, se ogni tanto non arriva un virus come si deve? :-)***

CONDIVIDE ET IMPERA

Salve a tutta la redazione.
Ho installato una skeda di rete e collegato i miei due PC con l'apposito cavo ma non so come trasferire i dati da un computer all'altro. Potete aiutarmi?

cellone88

▲ ***Due PC e un cavetto solo già una LAN!***

Supponiamo che tu abbia Windows XP su entrambi i PC, supponiamo che le schede di rete siano Ethernet, supponiamo che tu abbia utilizzato il giusto cavo incrociato (non un normale cavo di rete!). Devi solo attivare una connessione di rete utilizzando Start-> Impostazioni -> Connessioni di rete -> Installazione guidata rete e quindi condividere una cartella cliccando col pulsante destro su di essa e

attivando condivisione in Proprietà. Il trasferimento lo potrai così fare semplicemente trascinando gli elementi che ti servono nella cartella condivisa e recuperandoli sull'altro computer dalla stessa cartella (che raggiungi dalle Risorse di Rete).

BANCA BACCHETTONA

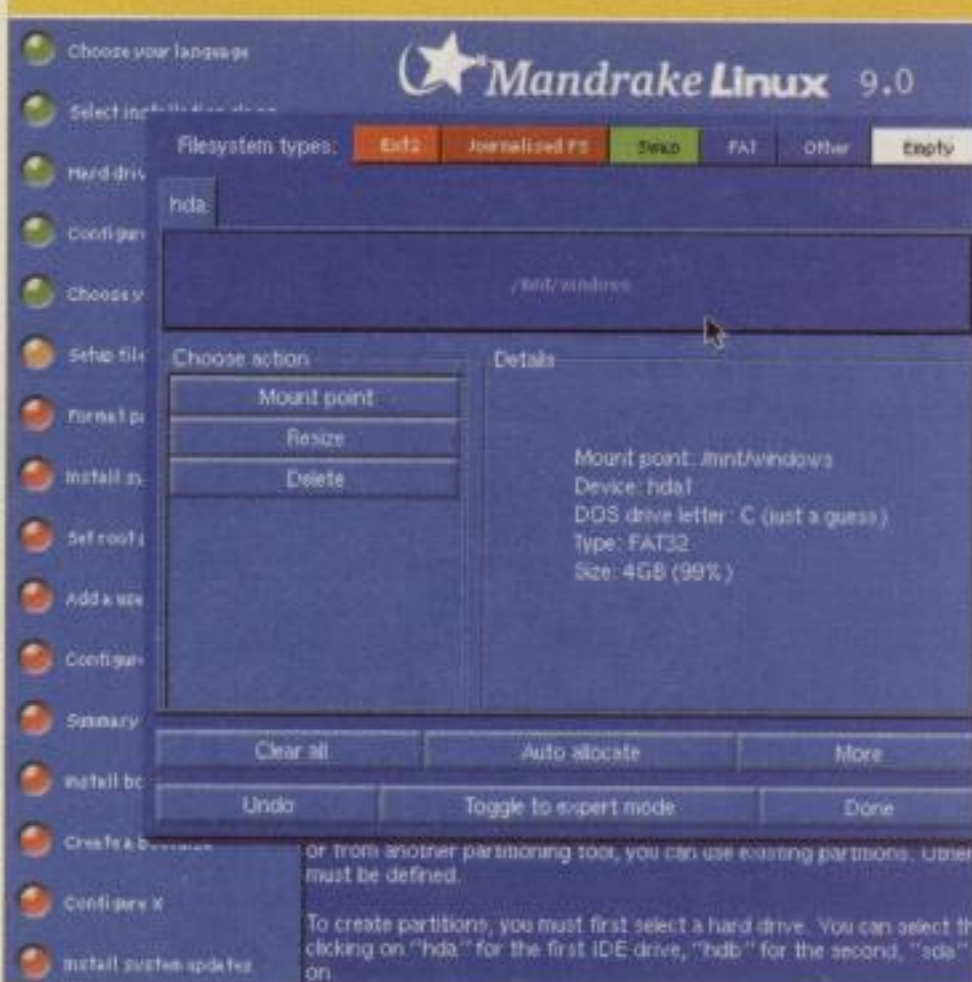
Spett. redazione,
vi voglio sottoporre un caso che riguarda la privacy e che mi è accaduto oggi. Mi reco presso la banca dove ho il conto corrente e noto che il sistema di accesso è cambiato. La nuova porta girevole con metal detector incorporato è simile alla precedente, ma noto la presenza di un monitor interno. Come al solito, il sistema rileva la presenza di qualcosa di metallico da me portato, (avevo lo zainetto con il portatile dentro), mi chiede di depositare gli "oggetti metallici nella cassettiera esterna", (chi non ha mai sentito questo messaggio alzi la mano). Primo inconveniente, la cassettiera non ha uno scomparto per zaini e borse, quindi rientro nella porta girevole per comunicare con un funzionario e chiedere il permesso di ingresso nella banca. Dopo varie insistenze da parte mia per accedere, (mi hanno chiesto se sono loro cliente, mi hanno detto che non si va in banca con uno zainetto e che bisogna presentarsi vestiti in maniera migliore, avevo jeans, maglione e scarpe da ginnastica, con un giaccone nero), mi danno il permesso di accesso, ma qua viene il bello. Il nuovo sistema, per farti accedere, comunica che occorre :"porre un dito sulla luce rossa e guardare il monitor"; anche il più idiota capisce che il sistema sta facendo una scansione delle impronte digitali e una foto digitale del soggetto, il tutto senza nessuna comunicazione all'utente e senza che io abbia firmato nessun tipo di autorizzazione, inoltre né all'interno della banca né all'esterno ci sono avvisi in merito.
Ho già fatto presente il caso al garante della privacy, ma volevo anche un parere da parte vostra, ricordando i vostri continui avvisi su violazione della privacy verificatasi in rete e non.
Sono pronto a ricevere qualsiasi tipo di consiglio su eventuali azioni, legali e non, da intraprendere.

Enzo

Qualcuno vuole rispondere a Enzo? A noi sembra che la questione più odiosa sia l'appunto del solerte funzionario sull'abito del cliente... Se così fosse, nessuno della redazione potrebbe mai più accedere a una banca... ;) Per il resto, un bel cartello all'ingresso con le spiegazioni del caso (e una cassettiera più grande) e tutto sarebbe stato risolto. O no? Fermo restando che io, personalmente, entrerei solo un'ultima volta in quella banca, per chiudere il conto.

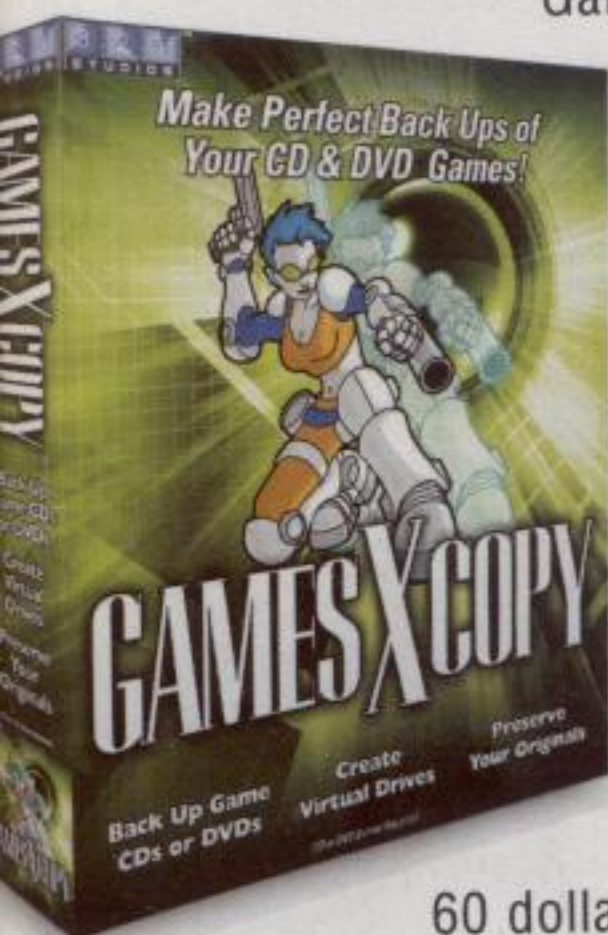
PARTIZIONE BILL

Ciao!
Io ODIO zio Bill (indi i suoi prodotti), e volevo passare a Linux, mantenendo però Win Xp (non sono l'unico utente del PC). Siccome quando ho comprato il computer (un paio di anni fa) non sapevo nemmeno aprire una cartella Win, quelli che me lo hanno venduto hanno allocato il 100% dello spazio sul disco per una partizione NTFS, contenente Win. C'è verso di disallocarne un pezzo (~ 10 giga su 60 totali, occupati 16) senza portare via pezzi al vecchio e bucato Xp? Come posso riallocarla da Win formattandola in ext3? Spero di non esser stato troppo invadente.

X-3ME'89
H4CK FROM TH3 R00TZ

Ciao a te!
Devi usare un programma apposito, tipo quelli di http://www.7tools.com/ o Partition Magic (ex Powerquest, ora di Symantec). Ricorda che puoi anche sperimentare Linux anche usando una distribuzione che funziona direttamente da Cd senza bisogno di essere installata, come Knoppix http://www.knopper.net/knoppix/index-en.html.

HOT!

BACKUPPARE GIOCHI

321 Studios (http://www.321studios.com/), una software house americana, ha presentato un programma, GamesXCopy, che permette a chiunque di creare una copia di sicurezza di un gioco o di qualunque altro programma e conservarla sul disco rigido del computer, se non registrarla su CD o DVD. Il software costa 60 dollari e funziona su qualsiasi versione recente di Windows. Chissà se copia se stesso. :-)

ANTISPYWARE PEGGIO DELLO SPYWARE

Il Center for Democracy and Technology (http://www.cdt.org/) ha presentato alla Federal Trade Commission statunitense un reclamo contro la pratiche di alcuni produttori di antispyware, che nell'intento di eliminare i programmi capaci di spiare la nostra navigazione su Internet o caricare pubblicità indesiderata sul nostro computer finiscono per fare più male che bene. Nello specifico ci si lamenta di Spy Wiper, un programma che di fatto, allo scopo di eliminare lo spyware sul nostro computer, ne installa di suo. Un'analoga iniziativa ha già fatto ritirare da Internet un'altra società, chiamata Spyban, il cui software era stato già scaricato da oltre 43 mila persone prima di venire messo sotto accusa. Attenzione, dunque: non basta che sia dichiarato antispyware, perché sia anche sicuro.

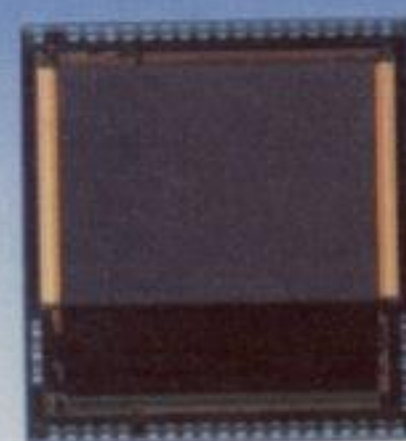
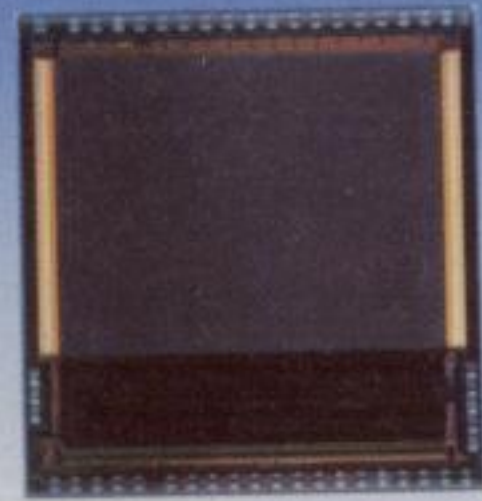
PERFINO LA NASA VA OPEN SOURCE

La NASA ha inviato alla Open Source Initiative (http://opensource.org) una bozza di accordo per fare dichiarare ufficialmente aperto il lavoro dell'ente spaziale americano. Se la OSI darà il suo benestare, potrebbe diventare pubblico, visibile da tutti e migliorabile da chiunque, anche il software che pilota un satellite o fa scattare le fotografie allo Spirit di turno. Il segreto, nel software, non fa comodo proprio a nessuno (Tranne che a Bill Gates).

ARRESTATA GIGABYTE, SCRITTRICE DI VIRUS

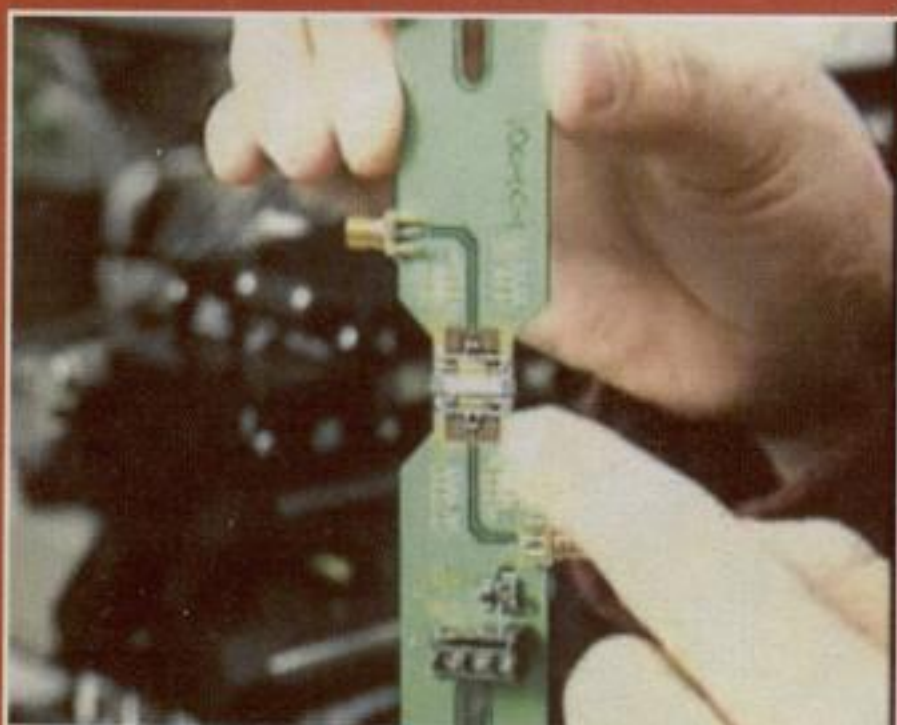
19 anni, conosciuta con lo pseudonimo di Gigabyte, è stata arrestata il 14 febbraio a Mechelen, in Belgio, davanti a casa sua. Creatrice dei virus Quis, Coconut, Sahay, Parrot e Sharp, o Sharpei, il primo virus scritto in C# di Microsoft .Net.
La polizia afferma che era pronta a pubblicare sul suo sito un nuovo virus, ora confiscato assieme ai cinque computer trovati in casa. È già stata rilasciata, ma rischia 3 anni e 200.000 dollari di multa.

UN MILIONE DI PIXEL IN 4 MILLIMETRI

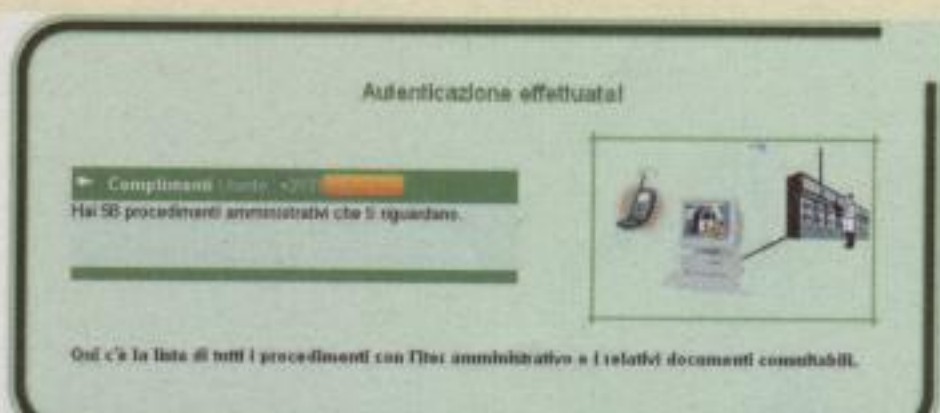
Anzi, di più. 1,3 milioni di pixel sono infilati in un rettangolino di soli 4,5 mm di diagonale: è la nuova microtelecamera vMAICOVICON di Panasonic. Il sensore è stato espressamente studiato per essere inserito nei nuovi telefoni cellulari, anche perché consuma un quinto degli attuali sensori CCD. Una bella rivoluzione, considerato che hanno già iniziato a produrne in quantità ed è già pronto anche il modello a 2 megapixel.

NON FACCIAMOCI FREGARE DAL VISUAL SPOOFING!

Ne inventano sempre una nuova... il visual spoofing consiste nell'usare accortamente link Javascript per lanciare una finestra di browser apparentemente normale, solo che alcuni suoi elementi grafici sono finti. Per cui la barra dell'URL sembra contenere un URL regolare e, sempre per dire, il lucchetto che contrassegna una transazione sicura in realtà è solo un'icona messa lì per fregare il malcapitato. Che, se ci casca, magari lascia lì il suo numero di carta di credito credendo di dialogare con una banca, o cose così. Sempre attenti e occhio vigile. Ci vuole poco a fare spoof. Chi non ci crede faccia una visita a http://www.docuverse.com/visualspoof/ per una dimostrazione pratica (innocua).

Sembra vero, eh? Possiamo capire che è un falso perché i tasti non funzionano.

VELOCISSIMI CIRCUITI LUMINOSI

1 GHz è la frequenza a cui Intel è riuscita a spegnere e accendere un raggio di luce in un dispositivo al silicio. La tecnologia è sensazionale, perché finora i sistemi per farlo così velocemente dovevano utilizzare materiali molto più costosi, come arseniuri di gallio e altre sostanze strane. Avremo comunicazioni ottiche velocissime ed economiche sia per collegare sistemi a fibra ottica, sia per far comunicare più velocemente i singoli chip all'interno del nostro PC.

AUTENTICATI COL CELLULARE

Si scrive il proprio numero di cellulare. Si clicca e si chiama il numero telefonico che appare. Uno squillo e la linea cade, per non pagare nulla e, soprattutto, per essere riconosciuti dal sistema.
Dopodiché si è autorizzati al login del sito Web dal proprio cellulare. Troppo semplice per essere vero? Provate il servizio presso http://pratiche.comune.venezia. it/indexkey.htm e vi chiederete perché non si è diffuso a macchia d'olio. Ce lo stiamo chiedendo anche noi.

HOT!

WEBBIT 2004 GRATUITO PER GLI ISCRITTI A GPI

L'Associazione Italiana Sviluppatori di Videogiochi - Game Programming Italia o GPI, vi farà entrare gratuitamente al Webbit 2004 se vi associate! Il Webbit è una manifestazione che si terrà a Padova, Milano e Bari, potenziale punto di incontro tra nuovi talenti, aziende e comunità del mondo dell'ICT.

GPI offre a tutti i suoi associati l'ingresso, una postazione PC e il dormitorio. Le date: a Padova il 6-7-8 maggio, a Milano il 3-4 giugno e a Bari il 21-22 ottobre. Per maggiori informazioni si deve contattare wergio@gameprog.it

MICROSOFT SI DISINTERESSA DEGLI UTENTI PER 200 GIORNI

Lo scorso 10 febbraio Microsoft ha finalmente riconosciuto ufficialmente l'esistenza di un bug in Windows che è stato scoperto il 18 agosto dell'anno scorso.
Quasi duecento giorni passati senza fornire alcuna comunicazione ai propri utenti è un bel record. Il bug non è esattamente una cosa da niente: Microsoft lo definisce critico per Windows XP, 2000, NT 4, NT Server 4 e Server 2003. Un attacco portato da un utente presente all'interno della rete in cui si trova la vittima potrebbe portare a un effetto banale come il controllo totale del computer attaccato. La soluzione è scaricare dal sito Microsoft le apposite patch. Certo, dirà qualcuno, in questi duecento giorni non mi è successo niente pur essendo a rischio, quindi sono al sicuro. Tanti auguri.

AUTODIS

Emergenza: occorre distruggere i dati, subito. Ma non è facile; ecco la pagella delle soluzioni migliori

Uno Stato di polizia. Dati compromettenti. Un'invenzione segreta da proteggere. Le vecchie lettere dell'amante. Quello che vogliamo. Bussano alla porta e in quel momento sappiamo che abbiamo solo pochi secondi per cancellare i dati in modo che nessuno possa metterci le mani sopra. Che facciamo? Ecco qualche soluzione, e i nostri voti.

Drag and puff

Tempo fa NukeLuke aveva uno script sempre pronto sul desktop, che in caso di bisogno avrebbe reso invisibile qualunque file trascinato su esso. Idea elegante, ma solo temporaneamente efficace e che non regge a una analisi attenta del disco (i file non vengono cancellati ma sono solo invisibili).

Eleganza: 3 - Efficacia: 1

Zero Write

Alfonso tiene sull'hard disk un programma di quelli che fanno secure write e scrive zeri su tutto il disco, in modo da cancellare rapidamente i dati per sempre in caso di bisogno. L'idea funziona ma c'è un avverbio di troppo: rapidamente. Mai provato a rasare a zero un disco rigido, diciamo, da sessanta Gb? Ci vogliono minuti interi, per fare un passaggio. In caso di emergenza i cattivi potrebbero staccare la corrente nel giro di pochi istanti, altro che minuti. Come dimostra l'esistenza delle Norton Utilities, i dati cancellati non sono irrecuperabili. Certi laboratori specializzati lavorano con tecniche sofisticatissime. Per esempio, il disco viene passato con un laser in grado di recuperare anche tracce flebili di dati. Ci sono laboratori che si vantano di poter recuperare dati da dischi che sono stati rasati anche set-

◄ *Un file cancellato non è mai per sempre, se chi lo vuole è sufficientemente determinato*

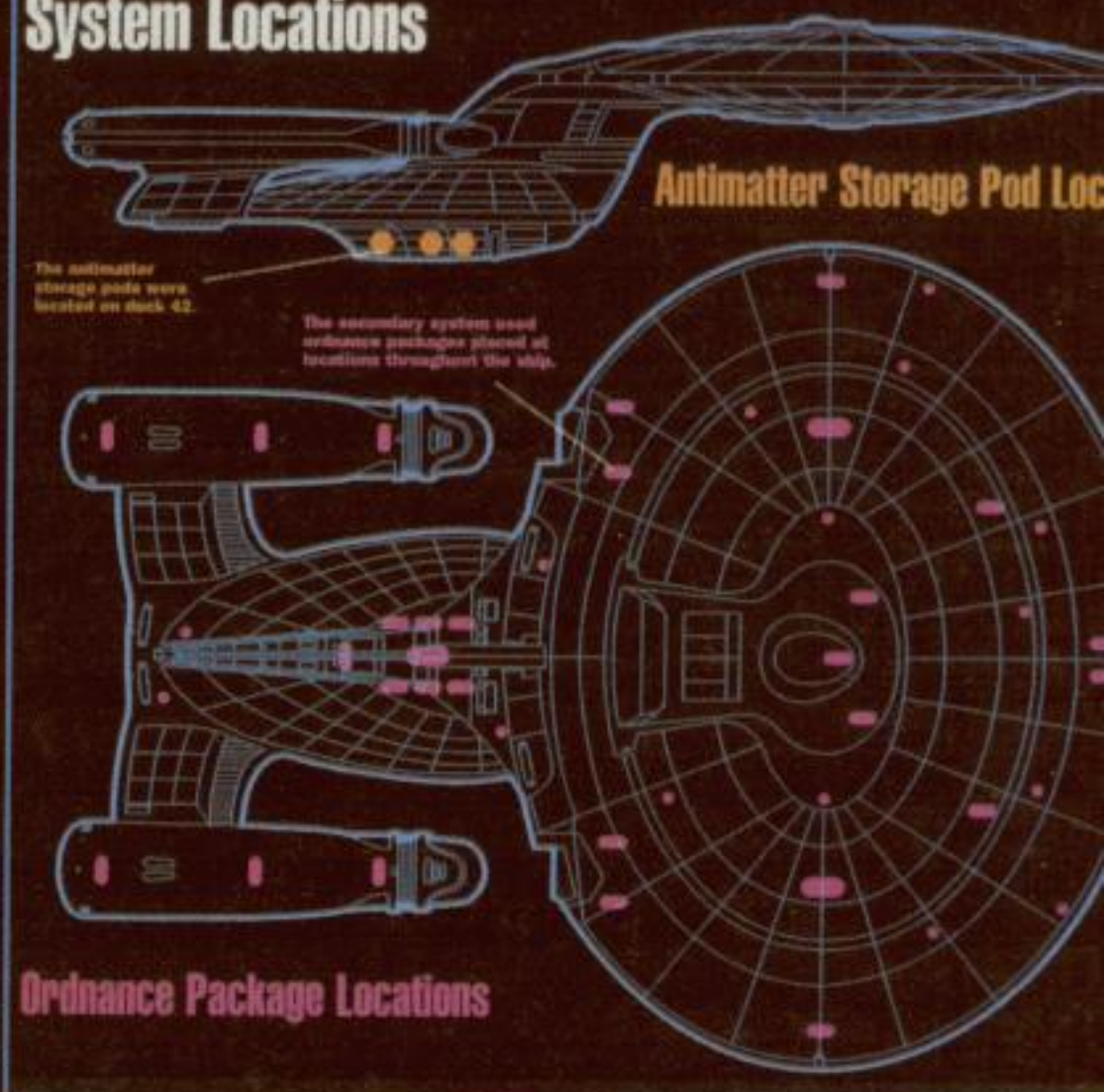
RUZIONE!

te volte! Per azzerare sette volte un disco da sessanta Gb non bastano ore, altro che emergenza. L'idea di un trucco software capace di agire in pochi istanti è affascinante, ma è anche pura fantascienza. L'unica soluzione sicuramente efficace passa dall'hardware.
Eleganza: 2 - Efficacia: 1

Carta canta (e sfrega)

Se si mette in conto di rendere inservibile il computer, o almeno il disco rigido, di idee ce n'è per tutti. Galile0, tecnico piuttosto esperto, ha aperto il suo disco rigido (operazione delicatissima) e ha allestito un ingegnoso meccanismo che tiene sospeso sopra il disco stesso un foglio di carta vetrata estremamente abrasiva. Dovesse verificarsi l'emergenza, gli basta dare un colpo abbastanza violento alla macchina perché il foglio cada sulla superficie e inizi a distruggerla.
Eleganza: 2 - Efficacia: 3

Cotto e smagnetizzato

Humanbean è un altro amante dell'hardware. Ha posizionato l'hard disk in mezzo a due bobine di rame, collegate a un relè, il tutto collegato a un timer, due batterie da 12 volt e a un grosso pulsante rosso. Se il pulsante rosso viene tenuto premuto per cinque secondi di seguito, il relè toglie la corrente al computer e attiva le bobine, che succhiano tutta la corrente fornita dalle batterie. Il disco rigido, in mezzo, viene contemporaneamente sottoposto al forte campo magnetico generato dalle bobine e al calore da esse generato.
Eleganza: 3 - Efficacia: 4

▲ *Se l'Enterprise possiede un sistema di autodistruzione, perché non potrebbe averlo il nostro PC? Magari non a base di antimateria...*

Sega a nastro

M4rth4 si è procurata, in forma portatile, uno di quegli apparecchietti che servono a cancellare al volo le audiocassette. È un degausser (sull'apparec-

IL PORTATILE CHE SI AUTODISTRUGGE

Si dice che il governo britannico stia producendo portatili i quali, se non aperti con il giusto codice, attivano un meccanismo in essi contenuto che li distrugge. I laptop così truccati andrebbero in mano ad agenti segreti e alte personalità con la tendenza a dimenticarsi il computer in giro. Fonti confidenziali affermano che attualmente Il Ministero della Difesa inglese perde più cinquanta portatili l'anno. E se ci fossero segreti di Stato?

chio c'è scritto Bulk Tape Eraser, ma è lo stesso), che sviluppa un campo magnetico molto forte, capace di creare una piccola apocalisse su qualsiasi superficie magnetizzata. Lo tiene sempre vicino al computer e le basterebbe un attimo per cancellare tutto.
Eleganza: 3 - Efficacia: 3

Colpo di tacco

A. è un commercialista milanese relativamente famoso nel suo mondo, specializzato, come dice lui, nella "riduzione del carico fiscale delle aziende". Genera dati di dimensioni ridotte – praticamente, alla fine, un'agenda, un database, un foglio di calcolo e qualche documento di testo – pochi ma preziosissimi ed estremamente confidenziali. Guai se cadessero nelle mani di un malintenzionato in grado di sfruttarli. La sua soluzione del problema è non tenere mai i dati sul computer. Si è comprato un paio di minicard Compact Flash e i suoi dati stanno tutti lì (avrebbe potuto essere anche uno di quei portachiavi USB che costano pochissimo). Il backup sta in una cassetta di sicurezza intestata a un amico fidato (talmente fidato che accetta di non averne le chiavi) e l'originale viaggia in un tacco delle sue scarpe. A. dispone di un terzo backup su un server raggiungibile via Internet e, quando aggiorna la situazione, fa viaggiare i dati, naturalmente dopo averli cifrati, all'interno dei pacchetti di ping. I trasferimenti sono ovviamente molto lenti, ma sicurissimi.
Su Internet girano milioni di ping ogni secondo, in tutte le direzioni, e chi potrà mai scoprire che cosa si nasconde dentro i suoi? Il nostro preferito.
Eleganza: 5 - Efficacia: 5

Memoria a breve termine

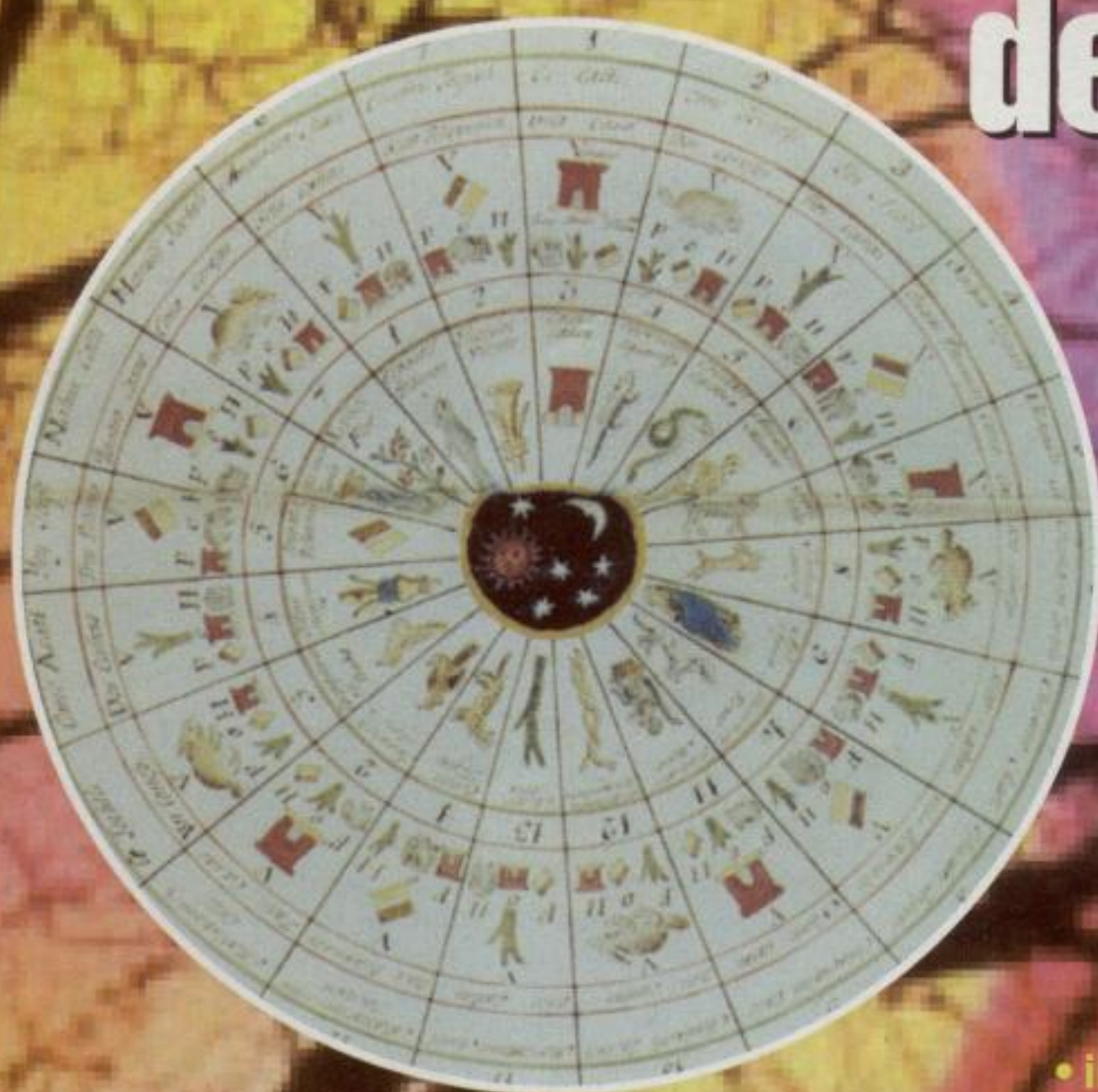
Il miglior modo per non avere dati a rischio sul disco, pensa fEdE, è non usare il disco! Quelle distribuzioni di Linux che funzionano da CD-ROM sono perfette come sistema operativo. Sull'hard disk si mettono le applicazioni che non stanno sul CD. Poi si gonfia il PC al massimo possibile della RAM (quattro Gb per un PC, otto Gb per un Mac) e si usa la RAM come disco virtuale. Niente di permanente. Certo, se bisogna riavviare, o se va via la corrente, è tutto perso. Ma la sicurezza ha il suo prezzo e fEdE ha un altro computer, che usa in modo normale, su cui mettere tutte le sciocchezze che non possono interessare nessuno.
Eleganza: 4 - Efficacia: 3

Il disco esterno

Tony lavora come amministratore di rete in certi uffici di Roma di una grande compagnia telefonica. Viaggia sempre con un disco esterno FireWire in tasca (ormai sono più piccoli dei palmari). I dati sono lì. Quando arriva in ufficio attacca il disco, e quando se ne va lo stacca. Tony ha contagiato Kya, la sua ragazza, con il virus della sicurezza. Kya ha un Mac e un iPod, che può anche funzionare come disco rigido esterno. Il Mac di Kya è completamente vuoto; il sistema operativo e i dati stanno tutti sul disco dell'iPod, che contiene anche tutta la sua musica preferita e dal quale non si separa mai.
Eleganza: 3 - Efficacia: 3

Qualcuno ha soluzioni migliori? Diverse? Originali? Siamo qui che le aspettiamo. :-)

Barg the Gnoll
gnoll@hackerjournal.it

Il GIORNO del GIUDIZIO

Solo i lameroni hanno bisogno del cellulare per sapere in che giorno della settimana cadrà il compleanno, o la festa nazionale, o la pizzata tra amici

L'unica cosa da imparare è che giorno della settimana è l'ultimo giorno di febbraio. Questo diventa il Giorno del Giudizio (GdG). In ogni mese pari n, il giorno n è il GdG. Quest'anno il GdG, l'ultimo giorno di febbraio, è una domenica. Quindi sarà domenica il 4 aprile, il 6 giugno, l'8 agosto, il 10 ottobre e il 12 dicembre 2004. Il 4/4, il 6/6, l'8/8, il 10/10 e il 12/12! Se ci chiedono che giorno sarà, per dire, Ferragosto, sappiamo subito che, se l'8 agosto è un GdG, anche il 15 – distante esattamente sette giorni – sarà come il GdG. Ferragosto 2004 sarà domenica: niente ponte :-(

I mesi dispari vanno a coppie. Il GdG è:

- il quinto giorno del nono mese
- il nono giorno del quinto mese
- il settimo giorno dell'undicesimo mese
- l'undicesimo giorno del settimo mese

Ossia sarà domenica il 9 maggio, il 5 settembre, l'11 luglio e il 7 novembre 2004, o 9/5, 5/9, 11/7 e 7/11.

Dal mese all'anno

Ogni anno il GdG slitta avanti di uno. Quando l'anno è bisestile, slitta di due. Il GdG 2003 era venerdì; il GdG del 2004, essendo il 2004 bisestile, è domenica (+2). Il GdG 2005 sarà lunedì (+1). Il GdG 2006 sarà martedì (+1). E così via. Ogni dodici anni il GdG avanza di uno. Per sapere il GdG di un qualunque anno del secolo scorso bisogna ricordare che il GdG del 1900 era mercoledì. Da lì si calcola come segue:

- **Prendere le seconde due cifre dell'anno (esempio: 1985 = 85)**
- **Dividere per 12 il numero di cui sopra e sommare risultato e resto (esempio: 85/12=7 con il resto di 1. 7+1=8)**
- **Dividere per 4 il resto ottenuto (esempio: 1/4=0 con il resto di 1) e aggiungerlo alla somma di prima (8+0=8).**
- **Togliere 7 o multipli di 7 se fa comodo. Esempio: 8-7=1. Aggiungere il risultato al mercoledì del 1900 per fare slittare il GdG. Mercoledì+1=giovedì. Il GdG 1985 era un giovedì.**

Altro esempio: in che giorno cadeva l'inizio del millennio, cioè il Capodanno 2001? Beh, il GdG 2000 era martedì. Quindi il 12 dicembre 2000 era un martedì. Ergo, erano martedì il 19 dicembre, il 26 dicembre e il 2 gennaio. Il primo gennaio 2001 era lunedì. Le stesse regole usate per il 1900 valgono anche per il 2000. In pratica abbiamo il sistema per calcolare a mente qualunque giorno del secolo scorso, di questo… e di qualsiasi altro.

Barg the Gnoll

◄ *John Conway: un uomo che sapeva come calcolare i giorni della settimana*

ATTENTO AL ci spiano

La tecnologia per sapere dove ci troviamo può servire anche per sapere dove possono trovarci...

Utile e divertente il GPS (Global Positioning System), per sapere dove ci troviamo, qual è la strada per andare alla festa dell'amica in campagna, orientarsi in campeggio e organizzare cacce al tesoro assai impegnative! Attenzione però alla sorveglianza indesiderata. In certe situazioni il GPS può fare correre grossi rischi alla nostra privacy.

GPS + GPRS = ?

Sappiamo che la tecnologia GPS non funziona per la sorveglianza di altri, ma serve a chi la usa per conoscere la propria posizione. Invece un cellulare GSM è poco meno di un radiofaro e si sa benissimo che, a telefono acceso, è tutt'altro che difficile per altri individuare la posizione dell'apparecchio. E arriviamo al punto: da un po' è iniziata la realizzazione di unità GPS che contengono anche un telefono cellulare (o telefoni con dentro un GPS, che è lo stesso). Supponiamo ora che il sistema sia composto in modo tale che il cellulare riceva periodicamente la lettura della posizione GPS e che invii altrettanto periodicamente a qualcuno un SMS con i dati stessi. Il qualcuno riceve i dati, li inserisce in un sistema suo e capisce al volo dove si trova il ricevitore GPS. Un telefonino più sofisticato, capace di collegarsi a Internet in GPRS, potrebbe anche fare a meno dei messaggini. Ora chiunque direbbe: "Ma il mio sistema non invia SMS a nessuno! E si collega a Internet solo quando lo dico io!" Sicuro? Proprio sicuro?

Categorie a rischio

In giro per l'Italia circolano migliaia di moto, auto e autocarri equipaggiati con un GPS di questo tipo. C'è un'ottima

GPS REDUX

Il Global Positioning System è stato messo in piedi dal Dipartimento della Difesa degli Stati Uniti a scopo militare. Attraverso i segnali che provengono da una costellazione di satelliti in orbita intorno al nostro pianeta si può conoscere la nostra posizione, velocità e direzione di marcia. Il sistema fornisce anche la misura dell'altitudine a cui ci troviamo. Ci vogliono i segnali di tre satelliti per calcolare una posizione. Meglio ancora averne quattro, situazione in cui il quarto funziona come sistema per la correzione degli errori. I sistemi GPS civili danno la posizione con un'approssimazione di circa venticinque metri. I sistemi militari, invece, sono assai più precisi e arrivano anche a qualche metro di risoluzione. Tuttavia il sistema di correzione differenziale GPS, cioè DGPS, consente anche in ambito civile di ottenere posizioni estremamente precise. Ci sono ricerche in corso per realizzare apparecchi che consentono ai non vedenti di orientarsi in città usando proprio questo sistema.

GPS in macchina. Bellissima cosa, ma attenzione alla privacy!

Un GPS da tasca, perfetto per orientarsi in qualsiasi situazione. Questo non ha problemi di privacy. Per ora...

GPS-GPRS:

Un satellite geostazionario come questo orbita per tutta la sua vita sopra lo stesso punto della Terra, a un'altezza di circa 26 mila chilometri. Per fare un sistema come GPS ce ne vogliono almeno venti, se non di più, per formare una costellazione simile a quella dei pentagoni cuciti sopra un pallone da calcio

ragione per farlo: un sistema che segnala costantemente la posizione di un veicolo è un antifurto eccellente e, per dire, permette a un corriere espresso di far conoscere al cliente lo stato della posizione e, letteralmente, la posizione del pacco da consegnare.
Sono così nate aziende che sfruttano il business e vendono servizi alle cosiddette flotte aziendali, ovvero i parchi auto e camion di aziende di trasporto, reparti vendita di grosse compagnie e organizzazioni con un gran numero di dipendenti che vanno in giro su una macchina della ditta. Queste aziende offrono l'installazione gratuita delle unità GPS-GSM, vendendola appunto come servizio utile in caso di furto del veicolo. Ci guadagnano sopra grazie al traffico telefonico e poi offrendo una serie di servizi, come la compilazione di registri di viaggio (quante volte ti sei fermato, dove, per quanto tempo, chilometri percorsi eccetera).
Ma il punto è che, spessissimo, chi guida questi veicoli non ha idea di se e quanto i suoi percorsi vengano sorvegliati e da chi, in azienda e fuori dall'azienda. Per gli agenti di commercio e i rappresentanti in genere al danno si aggiunge la beffa, perché spesso l'azienda chiede loro di partecipare alle spese di installazione del congegno in macchina! Morale: se nella nostra auto (o in quella di papà o mamma) esiste un impianto GPS aziendale, è possibile (e probabile) che ci sia dentro anche un sistema di segnalazione come quello che abbiamo descritto.
Saperlo è importante, non per fare i disonesti, ma perché abbiamo diritto di conoscere le informazioni che vengono prese sui nostri spostamenti e l'uso che ne viene fatto.

Reed Wright
reedwright@mail.inet.it

IL RIVALE GALILEO

Da tempo l'Unione Europea è al lavoro su un progetto, denominato Galileo, di un sistema alternativo al GPS e non americano, che svolga le stesse funzioni. Costerà oltre 230 milioni di euro e ci ha investito sopra anche la Cina, ma ancora non è chiaro quando potrebbe entrare in funzione, a parte la data ufficiale del 2008 fornita dalle autorità. Galileo impegnerà 30 satelliti, 27 operativi e tre di riserva, su tre orbite geostazionarie all'altezza di 26.316 chilometri da terra. Nel frattempo Usa e Unione Europea negoziano per arrivare a una compatibilità tra GPS e Galileo.

CHI LO FA DA TERRA

In tutto il mondo esistono oltre 1.100 radiofari GPS che trasmettono segnali da terra per correzione di errore e affinamento del segnale. La lista dei radiofari GPS italiani si trova all'indirizzo http://www.trimble.com/trs/findtrs.asp?Nav=File-14407&Detail=Italy.

IL GPS SUL NOSTRO PC

C'è chi lavora per integrare GPS e navigazione Internet. Il progetto GPSWeb aggiunge una intestazione User-Location a tutte le richieste in protocollo HTTP contenenti la posizione di un utente. In pratica, con un ricevitore GPS attaccato al computer e un plugin apposito per il browser, è possibile fare dialogare browser e GPS. Sul sito http://www.crs4.it:8000/gpsweb sono già disponibili una estensione per Mozilla e un daemon, GPSd, in Java, quindi universale per qualsiasi computer.

RAFFREDDAMENTO

Processori sempre più potenti hanno bisogno di dissipare grandi quantità di calore. Le normali ventole stanno diventando sempre più rumorose e allora perché non passare a un raffreddamento ad acqua?

Nei vari anni abbiamo assistito a una crescita esponenziale delle frequenze operative dei processori, doppiando la boa del Ghz nel 2000, 2 Ghz nel 2001 e 3 Ghz nel 2002. Insieme alla velocità è aumentato il calore da dissipare: se qualche anno fa bastava un rudimentale dissipatore in alluminio con una ventola 4x4 silenziosa, per raffreddare correttamente una cpu di ultima generazione sono necessari ben altri mezzi e soprattutto, ben altro rumore. Questo problema è accentuato dalla pratica del overclocking che porta a dover dissipare 100-150 W e oltre in soli 100 mmq circa. Ecco quindi comparire ventole tachimetriche 8x8 o 12x12 nei case, arrivando ad eguagliare per rumore un elicottero (dissipatori come il Volcano 11 fanno 74 db!). Parallelamente è andato sviluppandosi il raffreddamento ad acqua, che si basa sul principio della alta conduttività termica dell'acqua rispetto all'aria. Come è risaputo il silicio drogato è un superconduttore, ossia minore è la temperatura di esercizio, minore sarà la resistenza opposta al passaggio della corrente. Meno resistenza vuole dire anche maggiore overclockabilità. Per fare un esempio lo staff di Tom's Hardware Guide utilizzando l'azoto liquido a -199° è riuscito a portare un P4 Northwood C @ 5300 Mhz, ossia 2 Ghz in più rispetto alla frequenza nominale. Questa tecnica, come anche l'uso di anidride carbonica a -60°, non è adatta ad un uso quotidiano.

COME PER LE AUTO

I Componenti

I componenti fondamentali sono:
-uno o più WB (waterblock)
-un radiatore con una o più ventole
-un tubo
-una pompa di ricircolo e una vaschetta

Alcune premesse prima di addentrarci. Maggiore è la portata e minore sarà il tempo di ristagno del liquido caldo all'interno dei vari WB; inoltre una pressione sostenuta permette lo sfruttamento di effetti fisici come quello di Venturi, noto anche come paradosso idrodinamico. Sfruttando varie tecniche si può inoltre indurre il moto turbolento che asporta una maggiore quantità di calore rispetto al moto laminare. Fondamentale è anche la scelta del materiale impiegato: quelli generalmente usati sono rame, alluminio, ottone e plexiglas. Il plexy è solo per fronzoli estetici e non ha nessuna conducibilità termica; l'allumino e l'ottone conducono discretamente il calore ma il materiale col miglior rapporto prezzo/prestazioni è sicuramente il rame, che ha un coefficiente di conduttività termica doppio rispetto all'alluminio.
Il componente più importante in un sistema ad acqua è sicuramente il waterblock, che può essere a canaline (in genere 4 o 6) o ad alette, che si sono rivelate migliori. Esistono WB per CPU (con dimensioni di 50 X 50 mm o superiori), per GPU e Chipset (con dimensioni 40 X 40) e per hard disk (per prevenire danni da surriscaldamento di meccanica o di elettronica). Il waterblock viene fissato mediante staffe a vite o clip a 3 punti.

Il calore si diffonde in modo continuo nel metallo e viene asportato dall'acqua che passa attraverso lo scambiatore di calore. L'acqua viene fatta ricircolare mediante una pompa contenuta in una vaschetta (da mettere in sul fondo del case) oppure può essere esterna. Esistono anche vaschette di dimensione contenuta con 2 o 3 pompe per ottimizzare al massimo la portata nei sistemi complessi con più WB e più radiatori. Sono da preferire pompe con portata >700 lt/ora e con una prevalenza (ossia il massimo dislivello superabile) >160 cm. Il calore asportato dall'acqua durante il suo percorso attraverso il vari WB viene dissipato mediante un radiatore che ha dimensioni variabili da 16x 16 a "mostri" lunghi come la sommità di un case. Sul radiatore possono essere posizionate una o più ventole, in genere 12 X 12, tenute a basso voltaggio (e quindi molto silenziose) per evitare ristagno di calore tra le lamelle. Per collegare tra loro i vari elementi si utilizzano tubi di silicone oppure i tubi crystal trasparenti il cui diametro interno deve corrispondere a quello esterno dei raccordi dei WB. È consigliato usare tubi con interno 10/12 mm.

Come Scegliere il Materiale

Siccome la costruzione di una vaschetta e di un WB è ardua e quella di un radiatore veramente molto difficile, conviene acquistare prodotti già pronti. I migliori WB del mondo sono prodotti in Italia. I produttori più famosi sono sicuramente *Lunasio* (www.insanewb.com o www.lunasio-cooling.com); *Pctuner* (www.pctuner.net); *Wbhouse* (www.wbhouse.it) e *Oclabs* (www.oclabs.com). Ogni produttore ha a listino tutto il necessario per avere un ottimo sistema, compreso vaschette e radiatori. Se intendiamo utilizzare una tanica esterna come vaschetta, consigliamo l'utilizzo di pompe quali Sicce Nova, Sicce Idra, Seltz 20 o 30.

Quando montiamo il sistema per la prima volta, testiamolo fuori dal PC per scongiurare perdite (ricordiamoci di fascettare tutti i tubi) e poi inseriamolo dentro al PC. Il radiatore può essere messo sulla sommità del case e la vaschetta nel fondo del case, sotto i cestelli HDD. Un sistema raffreddato a liquido darà solo soddisfazioni e anche dopo 3-4 anni sarà perfettamente in grado di tenere a bada il calore dei nuovi processori. Considerando i vantaggi e la longevità, il rapporto prezzo/prestazioni è ineguagliabile!

Francesco Cariati

REGEX a

Scopriamo qualcosa in più in questo strumento essenziale per catturare informazione complessa da testi di grandi dimensioni

Qualche numero fa abbiamo lavorato al riconoscimento delle date, arrivando all'espressione regolare

```
[0-9][0-9]?[0-9]?[0-9]?[/._;-][1-9]|(0[1-9]|1[012])[/._:-][0-9][0-9]?[0-9]?[0-9]?
<-- anno o giorno -->        <--- mese ---->        <-- giorno o anno -->
```

Il mese è sostanzialmente a posto, ma è ancora possibile esprimere date assurde come 3333/11/4444. Uno dei due gruppi di quattro cifre potrebbe essere un anno, ma l'altro per forza non può essere una data! Il riconoscimento totale assoluto richiede tempo e lavoro quasi insostenibili, ma si può essere ancora più precisi e fare meglio.

<table>
<tr><th>STATE OF REGEX</th><th>STATE OF STRING</th></tr>
<tr><td><a>n(na|ts|nual)</td><td>the <a>nnual income</td></tr>
<tr><td>a<n>(na|ts|nual)</td><td>the a<n>nual income</td></tr>
<tr><td>an(<n>a|ts|nual)</td><td>the an<n>ual income</td></tr>
<tr><td>an(n<a>|ts|nual)</td><td>the ann<u>al income</td></tr>
<tr><td>an(na|<t>s|nual)</td><td>the an<n>ual income</td></tr>
<tr><td>an(na|ts|<n>ual)</td><td>the an<n>ual income</td></tr>
<tr><td>an(na|ts|n<u>al)</td><td>the ann<u>al income</td></tr>
<tr><td>an(na|ts|nu<a>l)</td><td>the annu<a>l income</td></tr>
<tr><td>an(na|ts|nua<l>)</td><td>the annua<l> income</td></tr>
<tr><td>an(na|ts|nual)</td><td>the annual< >income</td></tr>
</table>

La parola a Mauro

Mi chiamo Mauro, ho 14 anni e vivo a Bisceglie (in provincia di Bari). Vorrei provare a dare la risposta al quesito pubblicato sul n°43:

```
<-anno o giorno->
([0-9][0-9])|(0[1-9]|1[0-9]|2[0-9]|3[01])?[0-9]?[0-9]?[/._:-]

<-mese->
[1-9]|(0[1-9]|1[0-2])[/._:-]

<-anno o giorno->
([0-9][0-9])|(0[1-9]|1[0-9]|2[0-9]|3[01])?[0-9]?[0-9]?
```

Bravo Mauro!
Hai capito perfettamente il meccanismo. Puoi fare di più nell'esecuzione, però. La tua regex infatti cattura anche le date in forma scorretta.
Due gli errori fondamentali: la prima parte della regex cattura un numero da 00 a 99 e va bene per un anno, ma non per una data; inoltre l'operatore | (questo-o-quello) non va usato più volte dentro una parentesi.
Alcuni programmi lo accettano, ma altri no.
Meglio costruire con più parentesi e al massimo un solo | per parentesi.

Andiamo per gradi

Prima, mettiamo a posto l'anno. Questo può essere espresso in due cifre (04) o quattro cifre (2004). Il primo caso è semplice: vanno bene tutti i numeri da 00 a 99 (00 indica, per esempio, il Duemila). I numeri, per convenzione, sono sempre almeno due. Quindi:

```
[0-9][0-9][0-9]?[0-9]?
```

L'espressione è debole, ma poi unendola agli altri meccanismi di controllo basterà. Pensiamo a realizzare due regex distinte. La prima cerca anno-giorno-mese, la seconda giorno-mese-anno.
E poi potremo metterle una in alternativa all'altra con un operatore questo-o-

tutta FORZA

quello. Abbiamo l'anno, qui sopra. Abbiamo il mese, [1-9]|(0[1-9]|1[012]), che abbiamo sistemato nello scorso articolo. Abbiamo il riconoscimento del separatore, [/._:-]. Manca il giorno, ma lavorando sul mese ci si arriva in fretta: [1-9]|(((0[1-9])|([12][0-9]))|(3[01])). Una cifra da uno a nove, oppure – se la data ha due cifre – un gruppo da 01 a 09, un gruppo da 10 a 29, un gruppo da 30 a 31.

Possiamo scrivere allora la regex giorno-mese-anno:

```
([1-9]|(((0[1-9])|([12][0-9]))|(3[01])))[/._:-] ([1-9]|(0[1-9]|1[012]))[/._:-][0-9][0-9][0-9]?[0-9]?
```

Regex anno-mese-giorno:

```
[0-9][0-9][0-9]?[0-9]?[/._:-] ([1-9]|(0[1-9]|1[012]))[/._:-]([1-9]|(((0[1-9])|([12][0-9]))|(3[01])))
```

Questa-o-quella:

```
(([1-9]|(((0[1-9])|([12][0-9]))|(3[01])))[/._:-] ([1-9]|(0[1-9]|1[012]))[/._:-][0-9][0-9][0-9]?[0-9]?)|([0-9][0-9][0-9]?[0-9]?[/._:-] ([1-9]|(0[1-9]|1[012]))[/._:-]([1-9]|(((0[1-9])|([12][0-9]))|(3[01]))))
```

Collaudata sul file di prova che possiamo leggere nel riquadro, c'è di che essere soddisfatti. La regex funziona egregiamente con due soli problemi: 2222-11-6666 e 31-2-2004. È ancora possibile rilevare date troppo lunghe o illogiche. Il primo problema è risolvibile con accorgimenti (per esempio può servire cercare uno spazio all'inizio della data. Diversamente da quanto dice Jerk (grazie della mail!), rispetto al secondo problema non è impossibile lavorarci ulteriormente sopra e arrivare a un riconoscimento perfetto. Ma l'espressione diventa di lunghezza e complessità mostruosa. Chi vuole potrà provarci (è possibile), ma noi passiamo ad altro, perché ci sono ancora molte altre cose importanti da imparare in fatto di regex.

PROGRAMMI PER REGEX

Qualche esempio di programma per trattare espressioni regolari:

WINDOWS
The Regex Coach 0.6.0, freeware, http://weitz.de/regex-coach/

LINUX
^txt2regex$, open source, http://txt2regex.sourceforge.net
grep (nella shell)
È possibile trovare altri programmi cercando "regex" in http://www.linux.org nella sezione Applications.

Mac OS X
RegExTest 1.1, shareware, http://www.toolusersoft.com/
BBEdit, commerciale, http://www.barebones.com
grep (nella shell)

saper trovare le informazioni su Internet è la fonte del vero potere

Due domande per ripartire

Per il prossimo articolo, due domande. Una si può risolvere tranquillamente con gli strumenti fino a qui presentati: catturare gli indirizzi email all'interno, per esempio, di un enorme database di posta ricevuta. La seconda domanda è più intrigante. Supponiamo di avere questo file:

Brian Astin
Cate Blanchett
Christopher Lee
Elijah Wood
Ian Holm
Liv Tyler
Viggo Mortensen

Con un programma che permetta di fare ricerche e sostituzioni con le espressioni regolari, cerchiamo ([a-zA-Z]+)( )([a-zA-Z]+) e lo sostituiamo con \3\2\1. Che succede al file? Soprattutto, perché? Questo è un bel salto di qualità nel nostro uso delle regex. E ne approfitteremo per spiegare ancora altre cose.

Barg the Gnoll
gnoll@hackerjournal.it

DIVENTIAMO

Primi consigli per farsi una nuova vita, che nessuno conosce...

Chi darebbe le proprie informazioni personali a un vigile o un carabiniere? Praticamente chiunque, siamo obbligati! Chi le darebbe al primo sconosciuto che incontriamo in una chat? Praticamente nessuno, speriamo! Non dovrebbe neanche esserci bisogno di spiegare perché, se abbiamo passato il periodo di non-accettare-caramelle-dagli-sconosciuti.

Il passo successivo è diventare completamente anonimi sulla rete, in modo che nessuno, dal nostro collegamento a Internet, possa risalire a noi. Non è semplice ma standoci attenti si può fare e, alla lunga, diventa quasi una filosofia di vita: mai fare sapere chi si è e depistare qualsiasi tentativo di individuazione. Non parliamo qui di accorgimenti tecnici, ma di ingegneria sociale.

Atto primo: la Personalità

La prima cosa da fare è creare un altro se stesso, meglio ancora se più di uno. Mai vista su Internet la gente che fa finta di essere dell'altro sesso, o più grande, o di un'altra città? Ecco, impariamo da loro. Senza mollare la presa e stando bene attenti a essere credibili e non compiere passi falsi.

Come fabbricare una personalità credibile? Ma via Internet, ovvio! Visitando Geocities, Tripod, Yahoo e le altre comunità si hanno a disposizione infiniti dati su città, scuole, anni di nascita, curriculum scolastici e professionali e un sacco di altri dati praticamente da tutto il mondo. Non si tratta di rubare l'identità di un altro, ma ispirarsi alla vita della maggioranza delle persone. Più le nostre identità sono grigie e noiose, più funzionano. Studiare l'elenco del telefono della nostra città aiuta a farsi un'idea di quali siano i cognomi più comuni. Controlliamo con il Contacognome delle Pagine Bianche se il cognome che scegliamo è tanto o poco diffuso.

UN'ALTRO

▲ Rossi è un cognome diffusissimo

Sempre sulle Pagine Bianche (http://www.paginebianche.it) si possono scoprire anche i nomi, le iniziali, le firme più usate.

PAGINEBIANCHE.it
Facile trovarsi

Servizi e Curiosità

I nomi femminili e maschili più diffusi

Maria	387.131	Giuseppe	790.149
Anna	177.855	Antonio	549.966
Rosa	108.193	Giovanni	498.321
Giuseppina	107.716	Francesco	427.657
Angela	105.877	Mario	362.645
Giovanna	100.877	Luigi	360.648

I cognomi e le firme più diffuse

Rossi	67.994	Giuseppe Russo	2.772
Russo	47.581	Antonio Russo	2.273
Ferrari	39.221	Antonio Esposito	2.034
Esposito	34.104	Giuseppe Rossi	2.016
Bianchi	28.235	Salvatore Russo	1.773
Romano	26.214	Francesco Russo	1.706
Colombo	25.916	Giuseppe Esposito	1.672

Le iniziali più usate per i cognomi

in ordine decrescente:
C sono 4.131
B, M, P, S, D, G, F, T, A, L, R, V, Z, N, I, O, Q, E, U, K, W, H, J, X sono solo 3

Le iniziali più usate per i nomi propri

in ordine decrescente:
A sono 33.326
M, G, E, S, C, L, R, D, F, P, V, I, N, B, T, O, J, H, K, W, U, Z, Y, Q, X sono solo 406

I cognomi più lunghi

18 lettere - Tschurtschenthaler
17 - Pasquadibisceglie, Di Francescantonio
15 - Monterubbianesi, Mastrofrancesco, Mastroberardino
14 - Abbracciavento, Castrogiovanni, Canavacciuolo, Colafranceschi

I cognomi più corti

Bo, Pe, Po, Re, Wu, My, Mo, Hu.

Home Page | Ricerca per nome | Ricerche speciali | Servizi e Curiosità | Help

▲ Maria e Giuseppe sono di gran lunga i nomi più usati in Italia

Se la lingua non è un problema ci si può costruire un'identità straniera. I cinquanta cognomi più diffusi negli Stati Uniti, per esempio, si possono trovare su http://www.lifesmith.com/comnames.html. Tornando all'Italia, possiamo anche vedere dove questo o quel cognome è più diffuso, su http://gens.labo.net/it/cognomi/.

Un trucco molto comune consiste nel prendere a prestito l'indirizzo di una casa editrice trovato su un libro o su una rivista. Un altro trucco particolarmente efficace consiste nel fornire nazioni che non esistono più, come Jugoslavia, Cecoslovacchia, Repubblica Democratica Tedesca…

Oltre all'indirizzo fantastico bisogna recuperare almeno tre o quattro indirizzi del tutto reali, esistenti e concreti (anche se ovviamente non abitiamo lì!).

▶ Michelozzi: un cognome di origini toscane

SOLO PER TEORIA

Questo articolo parla di anonimato a scopo unicamente didattico. Per la legge italiana fornire dati personali falsi è ILLEGALE. Non confondiamo l'ipotesi di diventare anonimi, qui descritta, con il diventarlo veramente, che in molte situazioni può essere un REATO.

C'è chi non vuole essere riconosciuto, neanche su Internet. E sceglie l'anonimato

A cosa servono? Ad aprire un po' di account di posta elettronica gratuiti presso i provider preferiti. Gli account serviranno per tutte le volte che viene chiesto un indirizzo funzionante.

Atto secondo: il Personaggio

Il vero attore non prova rimorso a interpretare il cattivo. Allo stesso modo, non avremo rimorso a dare informazioni false a gente che tutto sommato mira ai nostri dati per profitto. Per questo, riempiamo i questionari con qualsiasi dato sia diverso dal nostro. Una tattica facile è scegliere sempre la prima casella, il primo menu, il primo pulsante.
In alternativa, quando c'è, scegliere sempre l'opzione Altro. Se non altro penseranno a come migliorare i loro questionari. Eccezione: è sempre bene fornire dati coerenti con il nostro indirizzo falso. Se "abitiamo" nel miglior quartiere di Roma o Milano, sicuramente abbiamo un ottimo reddito e una professione altolocata.

Crearsi un'identità virtuale per fare scherzi stupidi all'amico o al collega è da lamer

Atto Terzo: la Morale

Qual è il senso del vivere anonimamente? Non è vivere alle spalle degli altri (è illegale, è lame ed è stupido). Non è fare scherzi stupidi all'amico o al collega (durano poco e finiscono male). Non è evitare le tasse o la scuola (ancora più lame). È tenere alla propria privacy. Vanificare il lavoro dei produttori di spam e pubblicità indesiderata. Farsi rispettare anche da chi pensa solo ai soldi. Siamo nel Paese dove ogni giorno ci tocca dare un assenso al trattamento dei dati personali eppure alzi la mano chi non riceve email non richieste nella sua casella di posta. Se il Garante lavora come Lameron de' Lameroni, possiamo benissimo fare da soli. Vivere anonimamente è solo uno dei metodi possibili.

NeOkOn
neOkOn@hackerjournal.it

IL CODICE FISCALE

In Italia non può esistere identità anonima senza il suo bel codice fiscale. Generare un codice fiscale "autentico" a partire dai nostri dati immaginari è semplicissimo, perché esistono decine di siti e programmi che lo fanno per noi. Attenzione a non esagerare, ricordiamoci che fornire un codice fiscale falso è illegale! Qualche indirizzo rintracciabile al volo su Web:

http://www.webpool.it/cf/
http://www.codicefiscale.com/
http://www.comuni.it/servizi/codfisc/
http://www.mediameeting.it/codicefiscale.asp

LA CARTA DI CREDITO

Non è necessario acquistare con carta di credito in rete per essere anonimi, ma spesso i siti chiedono il numero unicamente a scopo di verifica e dissuasione. Non è difficile inventare un numero di carta di credito plausibile da soli: l'algoritmo è di dominio pubblico e lo esamineremo in un prossimo numero di Hacker Journal. Comunque sia ci sono programmi che lo fanno per noi, per esempio GenerID. Trovare numeri di carta di credito veri in Rete è facilino (Google indicizza anche fogli Excel…) ma NON VA FATTO. Uno, è un furto e i ladri difficilmente restano anonimi; due, è più facile che vengano effettuate ricerche di autenticità su quel numero. Non proviamo mai a usare i numeri di carta di credito inventati per comprare qualcosa: non funzionerebbe e ci metterebbe sicuramente nei guai!

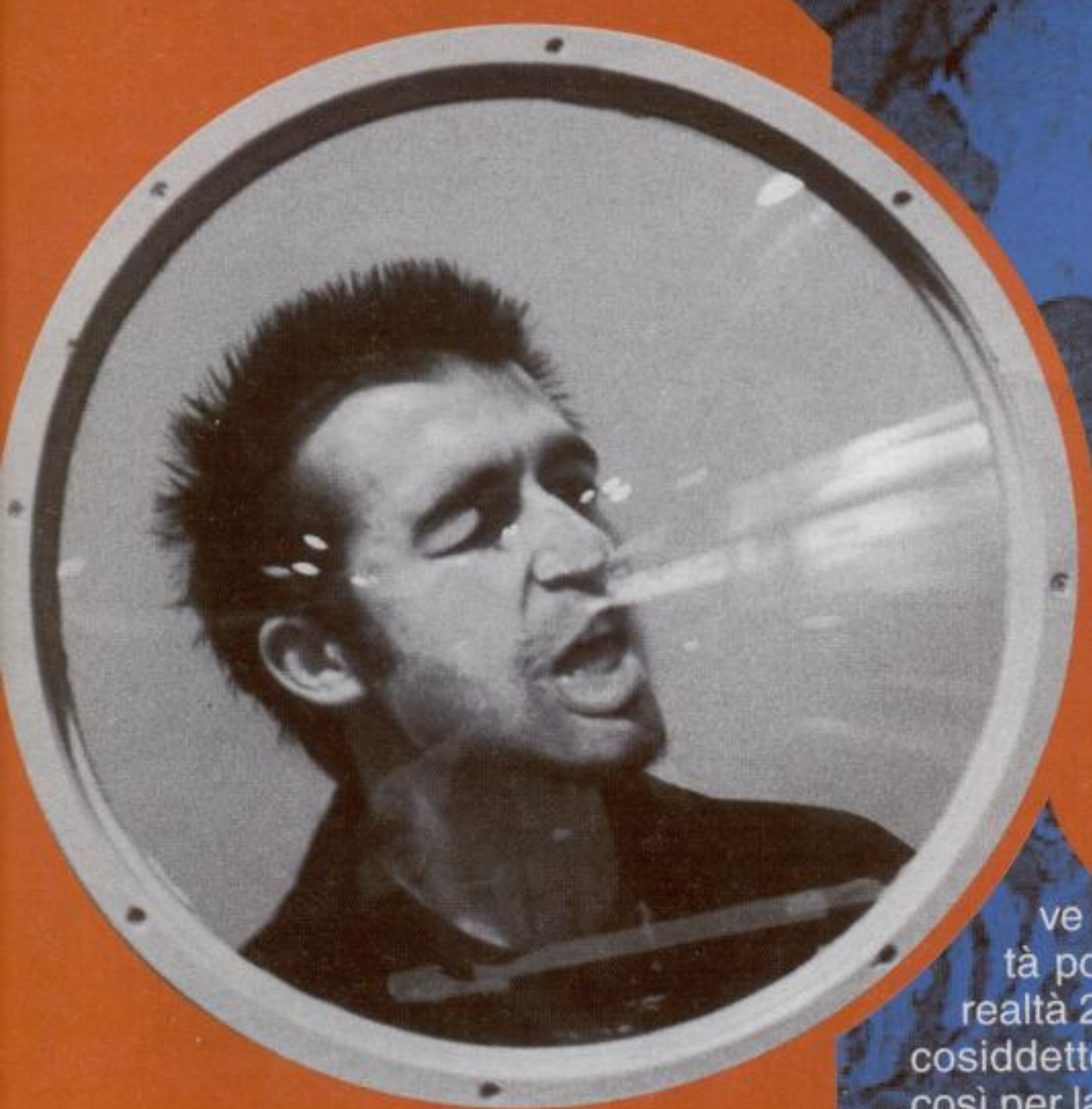
Ascoltare la POLIZIA

A caccia di frequenze proibite, senza nessuna esperienza e muniti delle nostre solite armi: PC e connessione

Lunedì, ore 12,57: una pattuglia ha appena svoltato l'angolo davanti alle vetrine di McDonald's. Un ragazzo di colore si gira con gli occhi stralunati e inizia a correre. L'agente accelera, è un attimo e gli sta davanti. Mentre il pilota chiama la centrale, il compagno sta già costringendo l'uomo a stendere le mani sul cofano. Una rapida perquisizione e poi l'invio delle generalità in centrale. "Ok, dammi il numero" "en-ai-uan-dabolou-seven-eigt…" "Ok, tenkiu. Nau wi cek…" e via, in diretta, in americano stretto, ma di cui captiamo l'essenziale.
Due minuti dopo la vita prosegue. Stessa pattuglia, stessa zona. È di nuovo controllo, è di nuovo scambio di numeri. Ora è lei che chiama, la voce femminile della centrale allenata alla tranquillità di fronte a ogni occasione, professionale, quasi confortante, tecnica quanto basta.

State ascoltando la polizia di New York, folks! Ed è in presa diretta all'indirizzo http://www.silive.com/policescanner/

Chi c'è dietro

Ma gli americani, naturalmente! È una battuta, ma fino a un certo punto. Non sappiamo in quale altro paese del mondo esista libertà sufficiente a consentire cose del genere: in Italia no, per esempio. Da noi è assolutamente vietato anche il radioascolto delle frequenze che, pure pubblicate sulla gazzetta ufficiale e quindi di dominio pubblico, consentirebbero di intercettare le radio dei servizi pubblici, polizia compresa.
Dopodiché, siccome la vendita di radio scanner è libera anche da noi (si, appunto, siamo in Italia…), tutto sommato se non ci si piazza proprio a fianco di un aereoporto militare e non ci si sofferma troppo a lungo sui cigli delle strade, ma per esempio si sta a casa propria, difficilmente qualcuno arriverà mai a controllare. Per il semplice fatto che il radioascolto non produce disturbi di nessun genere e che, si presume, non si metterà mai su Internet ciò che si è riusciti a captare. Già, ma qui sta il punto! La polizia di New York, invece, è proprio sulla rete, 24 su 24, 7 su 7! E con lei, in buona compagnia, anche i vigili del fuoco e praticamente tutte le stazioni di terra dei principali aeroporti degli Stati Uniti. Ma non è finita qui. Sono in linea perfino gli aeroporti militari, dai quali si possono ascoltare le conversazioni, parecchio tecniche, tra le torri di controllo e gli aerei in decollo e in avvicinamento. Roba da pazzi: o da ingenui, dirà qualcuno.
Ma è vero che ciò che si ascolta, senza nulla togliere al fascino della scoperta, è anche prevedibile. Vogliamo sperare che le vere trasmissioni critiche siano crittate tramite appositi scrambler, come avviene per la nostra polizia locale.

Bucare

Evviva WPA, abbasso WEP: la vecchia protezione delle stazioni di rete wireless era veramente debole: la sua chiave di cifratura aveva due modalità possibili, a 64 bit e a 128 bit. In realtà 24 bit erano sempre riservati al cosiddetto vettore di inizializzazione e così per la chiave rimanevano a disposizione solo 40 e 104 bit. Sono valori che andavano bene anni fa e non più oggi. Un malintenzionato poteva intercettare i segnali in arrivo e, con un po' di fortuna, riuscire a decrittare tutto nel giro di qualche ora. La nuova è meglio, ma qualche problema resta. Ecco perché.

WPA (Wireless Protected Access) e lo standard 802.11i danno la possibilità di usare chiavi di sicurezza cosiddette Pre-Shared, o PSK (Pre-Shared Key). Una PSK è composta da un numero a 256 bit oppure da una frase chiave (passphrase) lunga da 8 a 63 byte. Una stazione può avere un proprio PSK, ma non è detto.
Quando si usa una chiave Pre-Shared, essa costituisce anche la Pairwise Master Key o PMK, da cui deriva la gerarchia di chiavi Pairwise Transient Key (PTK). Il passaggio dalla frase chiave al valore di 256 byte necessario per la PMK è una semplice formula matematica, forse un po' troppo semplice.

La formula di PMK

Quando si usano chiavi Pre-Shared per generare PMK, ci sono due alternative: PSK come numero a 256 bit oppure come frase chiave. Nel primo caso la PSK viene usata direttamente come PMK; nel secondo, la frase chiave viene concatenata insieme al SSID e alla lunghezza del SSID stesso. La stringa così ottenuta viene hashata 4.096 volte per generare un risultato finale composto da 256 bit.
Per arrivare dalla PMK alla PTK il passo è piuttosto breve e si basa su una funzione che considera la PMK, i due MAC address delle schede che si parlano e i due nonce dei primi due pacchetti di handshake a quattro vie. Risultato: se la gerarchia delle chiavi è in possesso di qualcuno che possiede anche la chiave Pre-Shared, quel qualcuno ha accesso a tutta l'informazione di cui ha bisogno per fare danni.

Attacco ad ascolto

Si è capito che, per generare una PTK, un apparecchio deve disporre dei due MAC address necessari e dei nonce (oltre che del cifrario selezionato). Tutte queste informazioni sono contenute nello scambio di informazioni iniziale, che va dal primo comando ASSOCIATE fino all'handshake a quattro vie. Un apparecchio in ascolto può captare lo scambio

il WPA

di informazioni iniziale e, da lì, generare una PTK valida.

Attacco a dizionario

Una stazione che non conosca una chiave Pre-Shared basata su frase chiave può attaccarla offline. Infatti, una passphrase genera circa 2,5 bit di sicurezza per carattere. La sicurezza di una chiave è quindi di

sicurezza = 2,5n + 12

dove n è il numero di byte che formano la frase chiave. Per esempio, una passphrase di venti caratteri genera sicurezza di

2,5 * 20 = 50 + 12 = 62 bit

Sono veramente pochini. Una passphrase lunga venti caratteri o meno ha poca probabilità di durare a lungo sotto un attacco a dizionario eseguito a regola d'arte. Scommettiamo qualsiasi cifra che la rete wireless oggetto dell'attacco usa una passphrase più breve? Un attacco a dizionario effettuato offline contro l'hash prodotto dalla PTK durante l'handshake a quattro vie è predisposto al successo e, ci si creda o no, è un attacco più facile di quello condotto contro una vecchia, insicura, famigerata chiave WEP!

Salvi per caso

Le basi WPA sono dunque a rischio colabrodo? Mica detto. Una chiave Pre-Shared, si è detto, può anche essere un numero, casuale, di 256 bit.
Ebbene, una PSK anche di soli 128 bit è di fatto sufficiente a proteggersi dall'attacco contro l'handshake a quattro vie prima descritto. Probabilmente, contro un attacco a forza bruta, potrebbe bastare una chiave a 96 bit. Riassumendo: meglio un numero random di una passphrase troppo corta.

Da ricordare

I punti di pericolosità per una rete wireless, sia pure protetta da WPA, sono il fatto che chiunque sia in possesso di una chiave Pre-Shared può determinare una PTK semplicemente sniffando il traffico di rete e la vulnerabilità di una frase chiave troppo corta, diciamo sotto i venti caratteri, che consente di risalire in breve tempo alla PSK sfruttando un attacco a dizionario offline. Un attaccante che riesca in uno di questi due exploit può spacciarsi per membro della rete e mettere a rischio la rete stessa. Le chiavi Pre-Shared vanno bene solo per reti piccole, che corrono pochi rischi. Le altre usino numeri casuali al posto della passphrase, o siano consapevoli dei rischi che corrono.

Kurt Gödel
kurtgoedel@hackerjournal.it

GERGO HACKER (E NON)

HANDSHAKE
In inglese significa stretta di mano e indica il momento in cui due apparecchi stabiliscono il dialogo su una rete.

HASH
In programmazione, trasformazione di una stringa di caratteri in una chiave o in una stringa più corta di lunghezza fissa, che corrisponde univocamente alla stringa di partenza, e che per esempio semplifica il ritrovamento dei record in un database (è più facile e veloce cercare all'interno di stringhe più corte e di lunghezza univoca che non leggendo i record originali dell'archivio).

NONCE
Significa per stavolta, per adesso. Nella sicurezza informatica è sinonimo di number used once, numero usato una sola volta, tipico dei sistemi di autenticazione in cui si vuole evitare che le informazioni trasmesse in precedenza possano essere riutilizzate da un aggressore. Nel Regno Unito è anche una parola di gergo per indicare il pedofilo, quindi facciamo attenzione nelle chat!

PASSPHRASE
Una password costituita da più di una singola parola. Più la passphrase è lunga e complessa, meglio è. pippo è una pessima passphrase; l3 INIZIALi de11A Mya passphra5E f0rmano LA pAr014 IldMpfLI è una passphrase molto migliore, ma più difficile da ricordare.

SSID
Acronimo di Service Set IDentifier, identificatore unico a 32 caratteri attaccato all'intestazione dei pacchetti inviati su una rete wireless, che funziona come password quando un apparecchio mobile cerca di collegarsi.

Nokia ai NOSTRI ORDINI

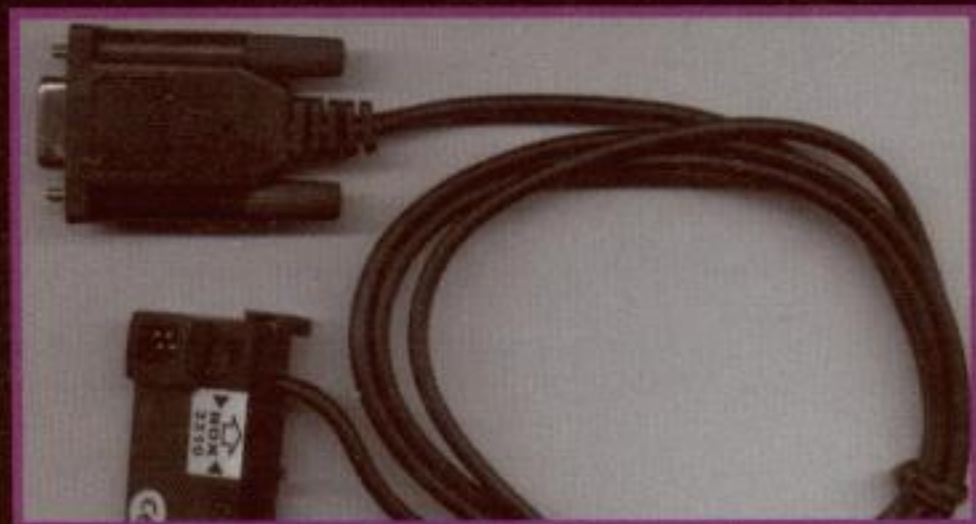
Collegare un cellulare Nokia al PC e ovviamente interagire con esso: ovvero mandare un SMS, backuppare la rubrica, verificare lo stato del telefono e molto altro

Per realizzare il collegamento servirà un cavetto seriale Nokia che ha un prezzo medio di 20 € - ma lo si può costruire cercando con un po' di buona volontà l'apposito schema nella rete - e la Nokia Data Suite 3.0 che servirà come interprete di comandi. Ovviamente ci vuole un briciolo d'impegno.

I test sono stati effettuati con il comunissimo Nokia 3310, ma funziona tranquillamente con molti altri cellulari: ne sono stati testati parecchi e tutti quelli che hanno la possibilità di collegamento seriale si comportano bene.

La Nokia Data Suite 3.0 aiuterà Windows a interpretare i comandi da noi inviati tramite l'installazione di un modem: infatti notiamo nella lista dei Modem la voce "Nokia GSM Data 3.0" e la sua relativa porta. Attenzione però: la porta indicata è puramente virtuale e la Data Suite si collegherà alla porta fisica specificata in fase di installazione.

Una volta aperto Visual Basic servirà un componente che permette di interagire con il modem Nokia installato precedentemente, componente che è il Microsoft Comm Control (MSCOMM32.ocx). Se per qualche strano motivo non fosse già installato, lo troviamo tranquillamente nel sito di Microsoft o in Rete. Il componente Comm Controll lo chiameremo "PortNokia" ed ecco qui di seguito il codice che permetterà l'interfacciamento con il Nokia, nonché i relativi commenti:

Con questo il collegamento al PC è un gioco da ragazzi

L'interprete del collegamento tra PC e cellulare sono i "Comandi AT" che permettono un interfacciamento semplice e veloce tramite codice ASCII. Penserà poi Windows a trasformarli in codice binario prima di mandarli al cellulare.

```
PortNokia.CommPort = 5 ' Selezioniamo la COM
  PortNokia.InputLen = 0 ' Impostiamo il valore di dati inviati uguale a 0
  PortNokia.PortOpen = True ' Apriamo la porta.
  If Err Then ' se è accaduto un errore lo notifico all'utente
    MsgBox "Impossibile aprire la COM" & PortNokia.CommPort & vbCrLf & Error$
  End If
  PortNokia.Output = "ATE" & Chr$(13) & Chr(10) 'Primo comando che mando al cellulare
```

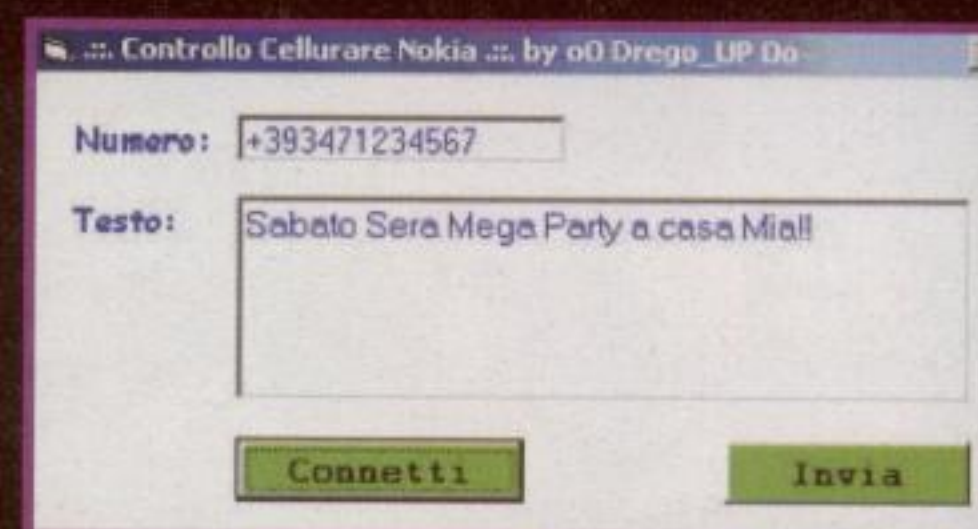
usando VISUALBASIC

fica la porta stessa e comunica con noi tramite una MsgBox, indicando la descrizione dell'errore restituito dal driver. Se il programma non restituisce nessun errore, allora si è sicuramente collegati al cellulare e la porta è aperta, ma bisogna dire al cellulare che si è presenti e lui dovrà rispondere "agli ordini". Per cui si invierà il comando ATE per comunicargli che si sta per sfruttarlo. La funzione chr$ restituisce un valore String che contiene il carattere specificato all'interno delle parentesi, per esempio Chr(10) restituisce un carattere di avanzamento riga, lo spazio.

In alcuni cellulari Nokia con la scritta "Accessorio Collegato" viene comunicato attraverso il Display che è stato effettuato il collegamento; in altri viene illuminato solamente il display e purtroppo in alcuni non viene comunicato assolutamente nulla, ci renderemo conto dell'avvenuto collegamento solo se risponderà. E adesso non resta che comandare il Nokia. Ecco la sequenza per mandare un solo SMS, ma è sufficiente applicare un ciclo for o while per consentire di inviare tutti gli SMS che vogliamo:

```
PortNokia.Output = "AT+CMGF=1"
& Chr$(13) & Chr(10)
PortNokia.Output = "AT+CSCA="
& Chr(34) & "+393492000200" &
Chr(34) & Chr$(13) & Chr(10)
PortNokia.Output = "AT" &
Chr$(13) & Chr(10)
```

Analizzando il codice vediamo subito che innanzitutto imposta la porta (ci si ricordi di impostare la porta virtuale che si trova indicata nel pannello dei Modem nella voce Nokia GSM Data 3.0). Successivamente, per evitare che un programma precedentemente chiuso abbia lasciato qualche dato ancora da inviare, si resetta la COM e si apre la porta con la proprietà PortOpen. Nel caso si verificassero degli errori la parte condizionale IF veri-

Il comando AT+CMGF=1 serve per comunicare al telefono che si devono impostare dei dati. Infatti nella riga successiva gli si comunica il numero del Centro Servizi utilizzato per inviare gli SMS: nel nostro caso si è utilizzato quello di Vodafone. Il comando AT serve solo per confermare i dati precedentemente inseriti e quindi salvarli.
Adesso non resta che indicare il numero di telefono e il testo; ecco come fare:

▲ *La schermata creata da VisualBasic: povera ma efficace*

```
PortNokia.Output = "AT+CMGS=" &
Chr(34) & txtNumero.text & Chr(34)
& Chr$(13) & Chr(10)
PortNokia.Output = txtTesto.text
& Chr$(13) & Chr(26) & Chr$(13) &
Chr(10)
```

Il codice è di facile lettura. In questo caso il comando AT+CMGS specifica la casella di testo contenente il telefono del destinatario e subito dopo il testo del SMS, la cui lunghezza non deve superare i 156 caratteri. Non necessitando di nessuna procedura di conferma, con Invio il SMS è già partito… Una cosa molto importate da ricordare è che, se dobbiamo mandare più SMS, dovremo aspettare 6 secondi tra un SMS e l'altro, poiché la maggior parte dei cellulari Nokia non permette l'accodamento degli SMS e quindi è da gestire con un semplice timer, che ogni 6 secondi invia un SMS prelevando il numero del destinatario dalla lista preparata. Il consiglio è quello di non impostare il limite dei 6" ma di aumentare un po' l'intervallo, per esempio impostando 10 secondi ed evitando cosi molteplici complicazioni tra le quali la congestione della rete. Si può trovare la lista completa dei comandi disponibili per i cellulari Nokia, tra i quali la lettura di SMS e rubrica all'indirizzo: www.oversoftware.net/nokia_hj.htm

Drego_UP
d.andrea@libero.it

Una telefonata da 10

"Pronto, sono Mike Hansen dell'ufficio estero della National Bank di Los Angeles, buongiorno" Ma siamo sicuri? E se fosse un impostore che vuole rubare informazioni? E se fosse... un ingegnere sociale?

Stanley Mark Rifkin, un attento lavoratore presso una società di software. 32 anni ben portati, un'intelligenza acuta, ottime capacità tecniche e, soprattutto, una curiosità senza fine. L'anno sotto esame: il 1978. Il luogo in cui ci troviamo: Los Angeles.

THE INSURANCE INSTITUTE OF LONDON{PRIVATE}

"INTERNET CRIME"

BY

OLIVER PRIOR

(Research Development and Knowledge Management, Willis)

Ora non esiste più, ma prima, proprio al centro di Los Angeles, sorgeva una grande palazzo che ospitava la Security Pacific National Bank. Rifkin aveva accesso alle aree limitate di tale edificio perché che era addetto alla configurazione di un sistema di backup dei dati del computer centrale della banca stessa. Un lavoro intrigante e delicato. Rifkin non ci mise molto a notare come gli impiegati, come quasi tutti gli impiegati del mondo poco attenti alla sicurezza delle informazioni riservate, ricevessero ogni mattina un foglietto con scritto il codice che dovevano utilizzare per la sala telex, cioè il codice di conferma per qualsiasi operazione bancaria. Ogni giorno un codice diverso, naturalmente. Questione di sicurezza, naturalmente... Non è difficile immaginare come da quella sala transitassero milioni di dollari, ogni sera, tutti i santi giorni, alla chiusura delle operazioni. Rifkin, con la scaltrezza che certo non gli mancava, riuscì a sbirciare un codice sul bigliettino, lasciato alla mercè di tutti, e fu così che gli venne in mente di studiare una strategia d'attacco.

Perché dovremmo imparare sofisticate tecniche di hacking, quando basta una telefonata?

Per quale motivo, si chiese, dovrei cercare di imparare tecniche di hacking o scaricare tool d'attacco dalla Rete impegnando lunghi giorni e lunghe notti su Internet, quando basta una telefonata per aumentare il proprio conto in banca di qualcosa come, diciamo, 10 milioni di dollari? Domanda all'apparenza ingenua, o alquanto strana, e forse priva di fondamenta, ma che invece è il punto d'inizio dell'ingegnoso meccanismo. O, se si vuole, dell'attuazione pratica di un'attività di social engineering. Non serve certo laurearsi per diventare un ingegnere sociale: piuttosto bastano una grande curiosità, spesso ottime capacità di persuasione, un bel po' di sangue freddo, coraggio, e a volte una spruzzata di

MILIONI di dollari

buona "parlantina" e di abilità nella gestione dei rapporti con altre persone.

L'attacco

È a questo punto che entra in azione Rifkin, aka Mike Hansen, dell'ufficio estero della banca. Da un telefono addirittura interno all'edificio della stessa Security Pacific National Bank, apre un conto alla Wozchod Bank di Zurigo. La tattica era quanto di più semplice si potesse pensare, almeno in teoria. Così, all'inizio di ottobre, osservò un impiegato che conosceva bene e ne carpì facilmente il codice di accesso a quella che aveva mentalmente ribattezzato 'la sala del tesoro'. In possesso di codice e di faccia tosta, si intromise in sala telex con la scusa di un controllo al software dell'host centrale. Impartire un ordine prestampato di trasferimento dalla cassa centrale al suo conto svizzero, di una cifra pari a 10.200.000 dollari, si è risolto in un digitazione, seppure con le mani che abbondantemente sudavano, di pochi numeri. Le informazioni riservate Rifkin-Hansen le aveva in mano.

Il trasferimento fu confermato. Pochi giorni dopo Rifkin volò in Svizzera per prelevare quegli spiccioli e gran parte di essi gli servirono per acquistare diamanti (che peraltro, successivamente, la banca ebbe non poche difficoltà a smerciare per recuperare almeno in parte il denaro sottratto).
A fatto scoperto, Rifkin entrò nel guinnes dei primati: aveva compiuto una delle più grandi rapine in banca senza utilizzare né pistole né computer: soltanto un telefono.
Ciò che lascia stupiti è il fatto che questa operazione venne considerata di puro hacking, tanto che il posto sul prestigioso libro dei top gli venne successivamente soffiato solamente, udite udite, da un certo Kevin D.Mitnick. Stupore che si può ben capire: un'operazione così, partita dalla scrupolosa pianificazione di un'attività di social engineering tanto cara a qualunque hacker, è però sfociata in una vera truffa a vantaggio del proprio interesse: e questo di hacking non ha certo granché. La fama, forse, nasce solo dalla morbosa partecipazione che tutti abbiamo nei confronti dell'intelligenza applicata, contro la stupidità routinaria di chi, invece, dovrebbe sempre stare all'erta.

Le informazioni riservate le aveva in mano, servivano solamente coraggio e sangue freddo in quantità

Il falso senso di sicurezza

È evidente che il nostro senso di sicurezza è troppo legato ai soli strumenti informatici. D'accordo, esistono oggi sul mercato imponenti software di difesa che permettono di garantire un adeguato livello di protezione dati, ma l'uomo resta sempre l'anello più debole della catena. Alla faccia di strumenti crittografici, software per il controllo dell'accesso, strumenti di autenticazione e quanto altro, un hacker abile e capace può perfino, per un momento, mettere da parte il computer e alzare la cornetta e… la beffa è consegnata!

Alone Sparrow

WHISKY E ICE, BABY!

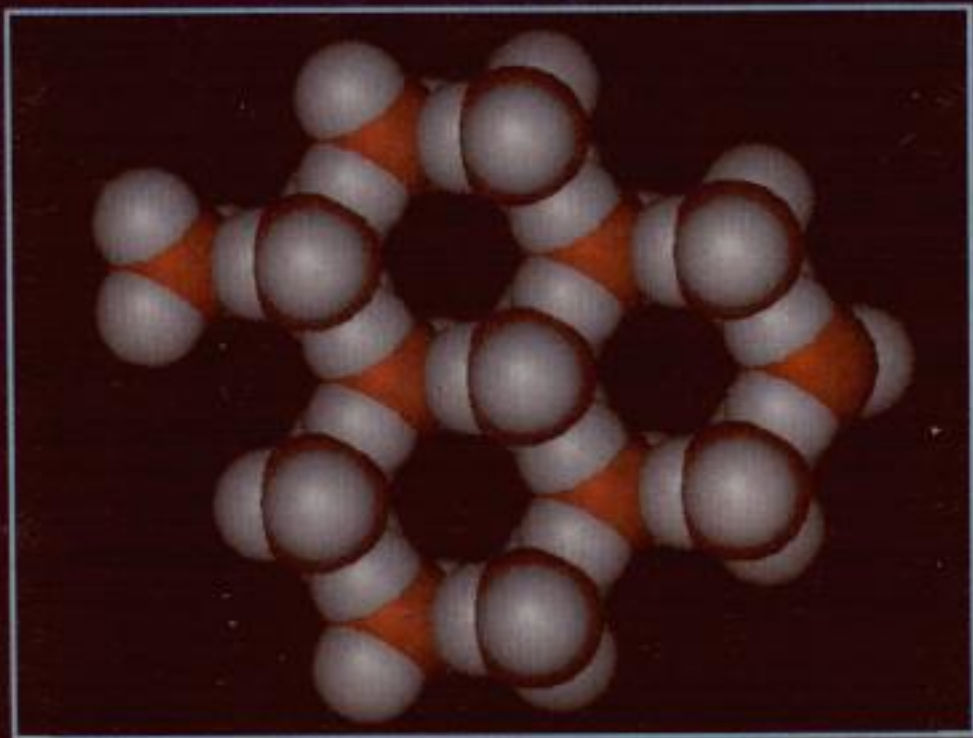
Come è fatto un algoritmo di crittografia

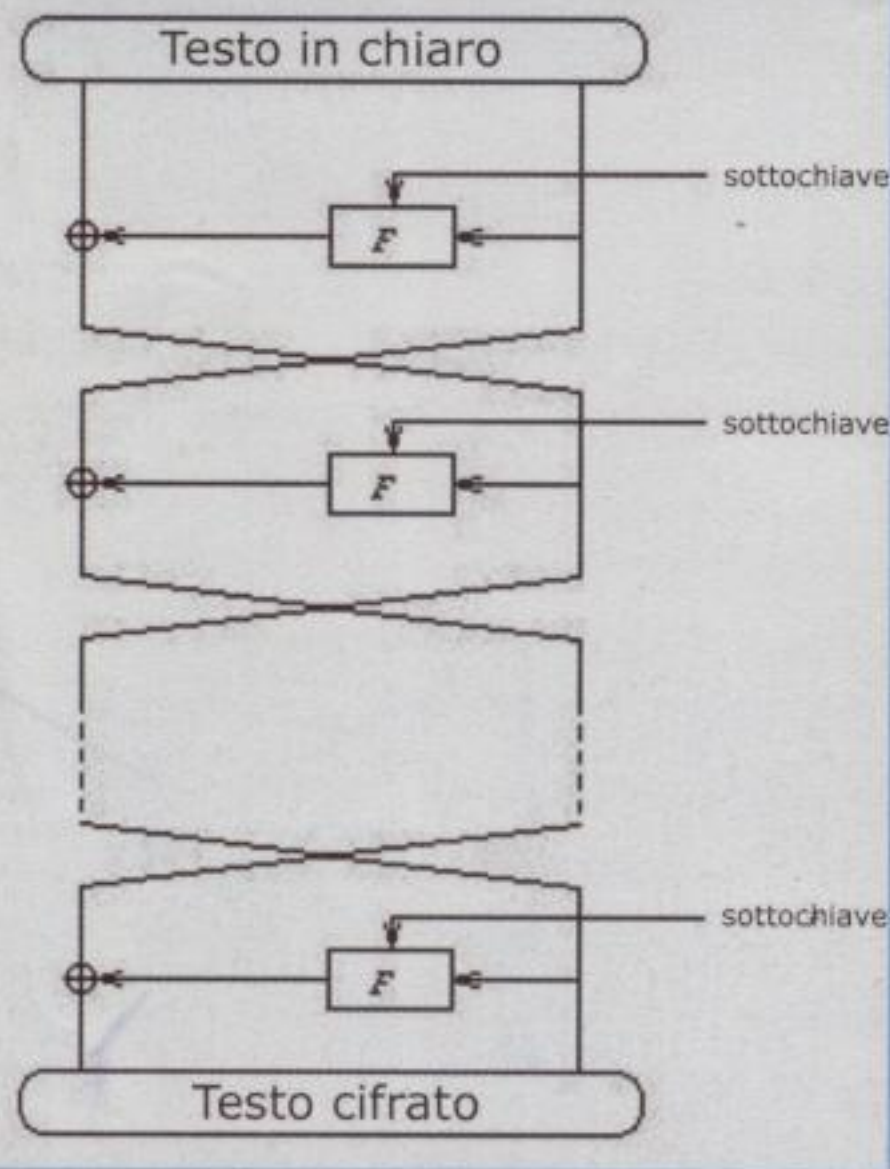
ICE sta per Information Concealment Engine (motore per nascondere informazioni). È un cifrario a blocchi a chiave privata a 64 bit, un po' come DES, IDEA o LOKI, che rimedia a difetti del DES come la vulnerabilità alla crittanalisi lineare e differenziale. Inoltre non ha chiavi deboli e la dimensione delle chiavi può essere qualunque multiplo di 64 bit, mentre DES si ferma a 56 bit. ICE è stato presentato nel 1997 durante la quarta edizione del Fast Software Encryption Workshop, da Matthew Kwan. Il trattato originale che descrive nei dettagli l'algoritmo si trova in formato PostScript compresso all'indirizzo http://www. darkside.com. au/ice/ice.ps.gz.

Le dimensioni contano

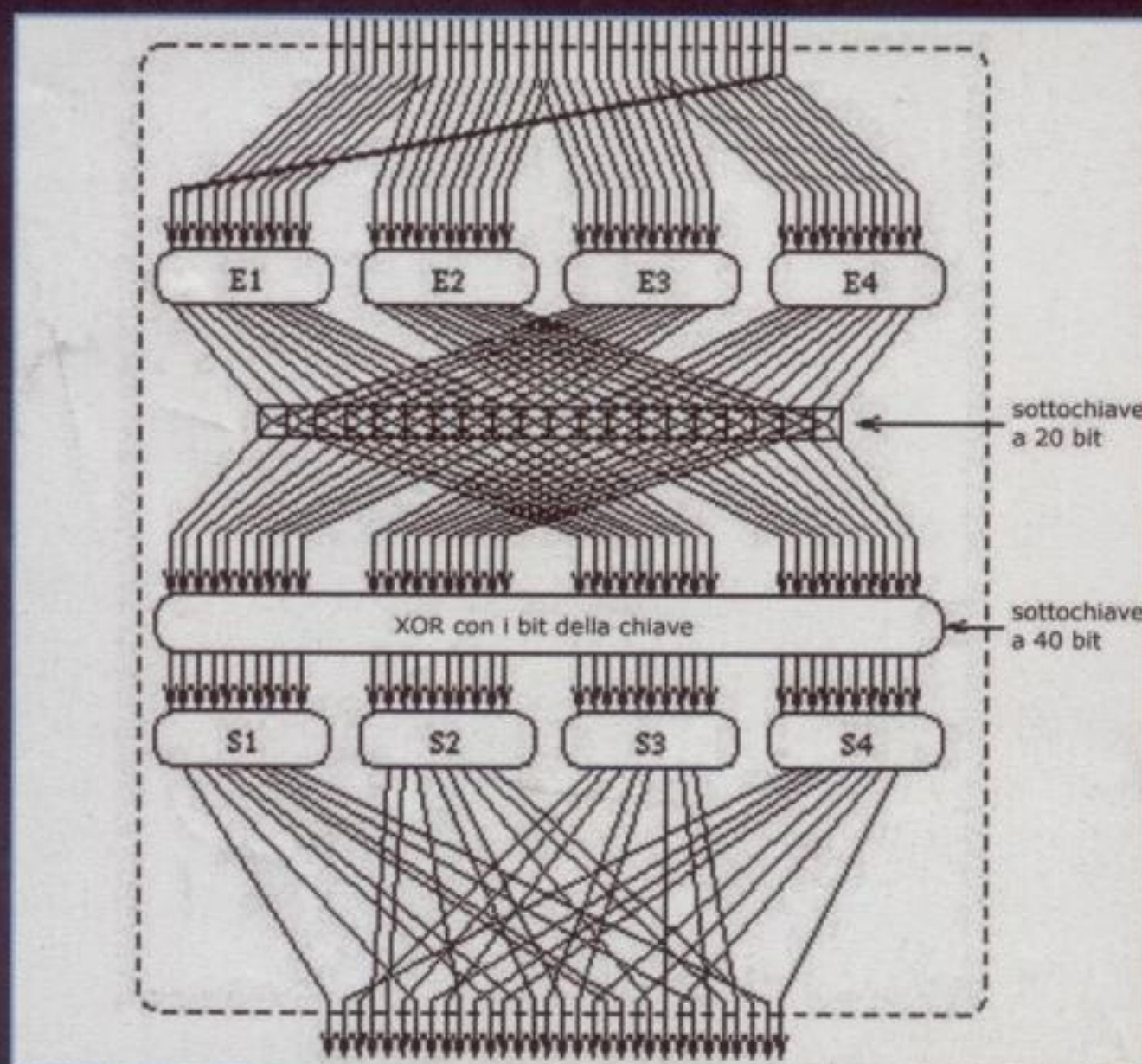
Se un cifrario è costruito bene, l'unico modo di violarlo è provare le chiavi una per una fino a che si trova quella giusta. Vuol dire che la dimensione della chiave determina il livello di sicurezza.

ICE ha più livelli di sicurezza. Ai livelli 0 (thin-ICE, come in ghiaccio sottile) e 1 (ICE) le chiavi sono lunghe 64 bit e una ricerca esaustiva nello spazio delle chiavi possibili richiederebbe mediamente la generazione di 2^63 cifrari. Il livello 2 utilizza chiavi a 128 bit, il livello 3 ha chiavi di 192 bit e così via. Più è lunga la chiave più è sicuro il cifrario, ma una chiave troppo lunga ha tempi di elaborazione inaccettabili e inoltre l'utente deve essere capace di creare, ma soprattutto ricor-

dare, password lunghe e complicate. Dal livello 2 in su si parla genericamente di ICE-n.

Come funziona ICE

ICE prende 64 bit di testo in chiaro e li suddivide in due metà da 32 bit ciascuna. La metà destra e una sottochiave da 60 bit vengono dati come input alla funzione F. Il risultato viene sottoposto a un XOR con la metà sinistra, dopo di che le due metà vengono scambiate. Questa procedura si svolge per un certo numero di volte, l'ultima volta non avviene lo scambio delle due metà. Il numero di volte dipende dal livello della cifratura: in Thin-ICE (livello 0) la procedura si svolge otto volte, mentre per gli altri livelli avviene 16 volte moltiplicato per il numero del livello. A livello 2, per esempio, avviene 16 * 2 = 32 volte.

Dal testo in chiaro al testo cifrato. Le due metà del testo in chiaro, a 64 bit per volta, e la funzione F vengono applicate più volte, rimescolando le informazioni fino ad arrivare al messaggio in codice

La funzione F

La funzione F è una complicata danza di bit, chiavi e sottochiavi, molto simile alla funzione usata in DES eccetto per la permutazione effettuata dalla sottochiave di 20 bit. Questi 20 bit decidono il percorso seguito dai bit in input. Se il bit della sottochiave ha valore 1, il bit corrispondente proveniente da E1 o E2 viene scambiato rispettivamente con un bit di E3 o E4. Se invece il bit della sottochiave è zero, non ci sono scambi.

La complessa funzione F prende un input di 40 bit e restituisce un output di 32 bit

Negli stadi S arrivano dieci bit in input e ne escono otto. I bit più a sinistra e più a destra dell'input vengono concatenati a formare un componente R da due bit, che contraddistingue quella parte di riga. Gli altri otto bit formano il componente C. Per ogni riga R il programma effettua un offset XOR (O) e genera un numero primo di Galois (P). L'output S finale deriva da

(C xor O)^7 mod P

Per una spiegazione più dettagliata la cosa migliore da fare è consultare il codice sorgente, disponibile a http://www.darkside. com.au/ice/ice.c.

La danza delle chiavi

Gran parte della sicurezza di ICE dipende dalla ripetizione delle funzioni di cifratura. Per esempio, in ICE livello 1 la procedura viene ripetuta 16 volte; ogni round usa 60 bit dei 64 bit della chiave, per cui ogni bit viene usato 15 volte. Quando un bit viene usato in un passaggio, viene invertito al passaggio successivo.

La forza di ICE

Come cifrario relativamente nuovo, ICE non è ancora stato sottoposto a una analisi rigorosa. Tuttavia, a detta del suo autore, un primo esame non evidenzia chiavi deboli o semideboli. Una chiave debole, se usata due volte di seguito, produce esattamente lo stesso risultato. Una chiave semidebole viaggia in coppia a una gemella e una delle due chiavi decifra l'altra. Per esempio, DES ha sedici chiavi semideboli note.

Sottoposto a crittanalisi differenziale, l'unica vulnerabilità potrebbe aversi su Thin-ICE, violabile tramite un attacco con testo in chiaro scelto e circa 2^56 cifrature. DES, a confronto, richiede 2^47 cifrature con lo stesso attacco. Altri metodi familiari di crittanalisi e di attacco non hanno evidenziato, per ora debolezze particolari. In attesa di verifiche più rigorose, ICE rappresenta quindi una ottima possibilità in più di produrre testo cifrato.

Chiunque lo voglia può scaricare tutti i file di ICE all'indirizzo http://www. darkside. com.au/ice/icepack.tar.gz.

Kurt Gödel

IL PROSSIMO NUMERO IN EDICOLA

25 MARZO 2004!

Guestbook!

Sognando il tuo computer del futuro, come lo vorresti?

Il mio computer del futuro?Lo vorrei integrato su un bel paio di occhiali da sole :-) **(KoMp4r3)** • Il computer del futuro? Come il mitico Nokia 9200 o il più moderno NEC e616 [cioè grande quanto un cellulare, con tastiera ed ampie connessioni wireless] **(danieleNA)** • Il mio computer dovrebbe essere veloce, affidabile e sicuro, cioè LINUX! Anche il case potrebbe essere a forma di Tux! **(Valkiry)** • un computer perfetto sarebbe un portatile con un win che non va in crash **(Angel)** • Magari trapiantato nel mio cervello, e leggere i DVD passandoci sopra con le dita !!! **(Th3^Cr0W)** • Senza limiti, e magari con un SO creato da me, "Cr0w Professional" !!! **(Th3^Cr0W)** • il pc del futuro dovrebbe usato con dei speciali occhiali che ci proietterebbe dentro al pc, cosi' sarebbe più facile programmare e imparare più velocemente l'uso del computer **(MAX343)** • ...il mio computer del futuro?...veloce, decisamente più veloce... **(Miles Underground)** • bello e veloce come un mac, sicuro-stabile-ecc|ecc come unix (ok, c'e' gia' e' macintosh OSX) ma anche diffuso come windoze. e basta. Grazie per il vs. lavoro e ciao **(zerinol)** • vorrei un computer intelligente.........ma non più di me !!! **(VIVINC)** • biprocessore: normale e ottico,hardware normale, sistema operativo:lindows **(amstrong)** • beh lo vorrei com almeno 10 gb di ram così si comincia ad usare windows dignitosamente..W LINUX! **(Offdexter87)** • Mhhh....un 10000 Ghz , 10000ram ddr a 5000mhz, skvideo GeForce10 Ti 15800 2048 ddr, HD 500 gb e poi una connessione da 100mb/s come standard al posto della 56kb =)) **(ovvHe)** • A dire il vero a me va bene anche così, cmq lo vorrei completamente programmabile (proprio in tutto)... E con un sistema operativo programmato solo dall' utente, così tutti sanno come funziona VERAMENTE l' OS dei propri PC! **(The_Shadow)** • Vorrei che il riconoscimento delle periferiche (ma anche dell'hardware in generale) fosse sicuro e standard. Vorrei che tutto il "ferro" che c'è sulle nostre scrivanie fosse indipendente dal SO che usiamo. credo che basterebbe definire un linguaggio che svolga la funzione di configurare ogni elemento hardware della macchina in modo automatico: magari inserendo questa sorta di script direttamente sul componente. Certo, bisognerebbe dotare ogni bios di un interprete per questo nuovo linguaggio in modo da permettere la sostituzione di QUALSIASI pezzo senza doversi preoccupare della compatibilità col SO o di dedicare tempo e energie a raggiungere una configurazione accettabile. Vorrei anche che i "pezzi di ferro" non fossero soggetti a surriscaldamento. Vorrei delle schede madri dove non passa corrente ma raggi di luce: impulsi che viaggiano alla velocità più alta che conosciamo. Sicuramente trovare una tecnologia che sia più veloce di quella che sfrutta la velocità della luce richiederà mooolte energie. Per lo meno ci ritroveremmo con un "qualcosa" che non sarà superato nel giro di 12 mesi. Grazie per aver letto fino alla fine. Grazie per darCI continuamente "nuovi stimoli positivi". Grazie per avere la voglia di pubblicare questa mail ma non lo spazio per farlo (...e non sono ironico, so che ho scritto un papiro) TNK! **(emme)** • Bè a questa domanda vorrei dire la mia: visto che io amo il mio computer, il computer del futuro vorrei che avesse la figa! :-) **(badboy84)**

SUI PROSSIMI NUMERI...

una sorpresa! Vi diremo tutto e... attenti alla sfida!

...ma continuate a farci avere tante email con tanti spunti interessanti!
guestbook@hackerjournal.it

hackerjournal.it

il muro per i tuoi graffiti digitali